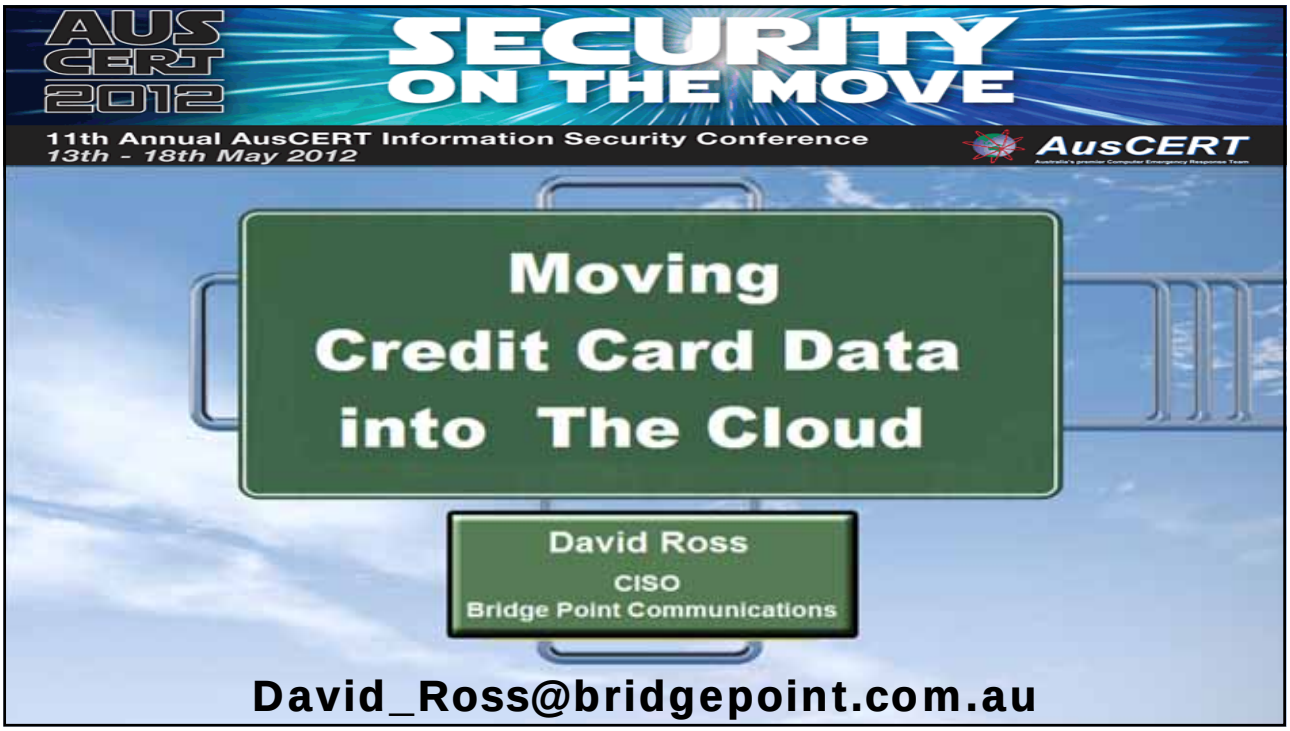


Agenda

- The Cloud Security Information Fountain
- The Payment Card Industry Data Security Standard
- PCI + Virtualisation
- PCI + Private/Virtual-Private/Dedicated Clouds
- PCI + Public Clouds – “PCI” and non-PCI compliant
- Cloud Security Alliance – Australia Chapter

UNCLASSIFIED

BRIDGE POINT
"SECURE NETWORKING"

Slide 2

Note!

- I AM a PCI QSA.
- If I am NOT YOUR QSA then the contents of this presentation can NOT be taken as PCI advice.
- YOU must consult with YOUR QSA to determine the relative merits of YOUR particular situation to determine sufficient controls to ensure compliance.

UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 3

QSA's really are assessed too...

Q **What is the Council announcing?**

A *Effective immediately, the Council is announcing the revocation of [redacted] status as a Council Qualified Security Assessor (QSA) and Payment-Application Qualified Security Assessor (PA QSA).*

Q **When is this revocation effective?**

A *This revocation is effective immediately, August 03, 2011.*

Q **Why is this revocation happening?**

A *[redacted] status as QSA and PA-QSA is being revoked due to the company's failure to meet the high standards demanded of QSAs and PA-QSAs.*

UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 4


CLOUD SECURITY = HOT TOPIC
Image: **Jan Smith** (Brisbane, Australia) *One Bright Cloud*


Cloud security current research
PROTECT
Cloud Computing Security Consid
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Special Publication 800-
CSA cloud security alliance
Guidelines on Security and Privacy in Public Cloud Comp
Wayne Jansen
Timothy Grance
SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0

Payment Cards are also a hot topic

- Jun 2005 CardSystems Solutions ~40 million cards
- Jan 2007 TJX Companies Inc. up to 90 million cards
- Jan 2009 Heartland Payment Systems ~130M cards
- May 2011 Citigroup ~360,000 cards
- …then 8 weeks ago…

Payment Cards are also a hot topic

globalpayments

kpn

Image: CC by Flickr user bearclau

PCI Security Standards Council

BRIDGE POINT "SECURE NETWORKING"

Slide 9

PCI Data Security Standard

- "PCI DSS" Version 2.0 (October 2010)
- 12 High-level requirements:

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

PCI DSS and Assessments

- Highly prescriptive
- 12 High-level requirements
- 198 Detailed requirements (194 if not hosting provider)
- 297 Audit Test Procedures (289 if not hosting provider)
- **1063** (**1004**) Items of Evidence to be reported in ROC

For example...

PCI DSS Requirements	Testing Procedures	
Requirement 1: Install and maintain a firewall configuration to protect cardh		
1.1 Establish firewall and router configuration standards that include the following:	**1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following:	
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.	• Identif i. Te ii. Ap iii. Te iv. Ap

Some have multiple test procedures

PCI DSS Requirements	Testing Procedures	ROC Reporting Details (For In-Place Requirements)
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**2.1.1** Verify the following regarding vendor default settings for wireless environments:	
	2.1.1.a Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions	• Identify the document requiring that wireless encryption keys must be chan i. From default at installation ii. Anytime anyone with knowledge of the keys leaves the organization o • Identify the responsible personnel interviewed who confirm the documente changing keys are followed: i. At installation ii. Anytime anyone with knowledge of the keys leaves the organization o • Describe how observed wireless configurations confirm that key changes ar required.
	2.1.1.b Verify default SNMP community strings on wireless devices were changed.	• Identify the document requiring that default SNMP community strings must • Describe how observed wireless configurations confirm that default SNMP are changed.
	2.1.1.c Verify default passwords/passphrases on access points were changed.	• Identify the document requiring that default passwords/passphrases on acc changed. • Describe how observed wireless configurations confirm that default passwo changed.
	2.1.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over	• Identify the document requiring that firmware on wireless devices must be strong encryption for: i. Authentication

And many items of evidence each...

ROC Reporting Details (For In-Place Requirements)	Reporting Methodol			
	Observe system settings, configurations	Document reviews	Interviews with personnel	Observe process, action, state
• Identify whether any insecure services, protocols or ports are allowed. • For each insecure service, protocol and port allowed: i. Identify the documented justification. ii. Identify the responsible personnel interviewed who confirm that each insecure service/protocol/port is necessary. iii. Identify the firewall and router configuration standards which define the security features required for each insecure service/protocol/port. iv. Describe how observed firewall configurations verify the security features are implemented. v. Describe how observed router configurations verify the security features are implemented.	✓	✓	✓	
• Identify the firewall configuration standards that require a review of firewall rule sets at least every six months. • Identify the router configuration standards that require a review of router rule sets at least		✓		

Little in print on PCI in the Cloud

PCI Security Standards Council

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessme

PCI Security Standards Council

Standard: PCI Data Security Standard (PCI DSS)
Version: 2.0
Date: June 2011
Author: Virtualization Special Interest Group
PCI Security Standards Council

Information Supplement:
PCI DSS Virtualization Guidelines

Except for vendors...

What Amazon Web Services product offerings support st
transmission of credit card data?

Services that support the processing, stora
provider have been validated as being comp

- Amazon Elastic Compute Cloud (EC2)
- Amazon Simple Storage Service (S3)
- Amazon Elastic Block Storage (EBS)
- Amazon Virtual Private Cloud (VPC)
- Amazon Relational Database Service (RDS
- Amazon Elastic Load Balancing (ELB)
- Amazon Identity and Access Management (
- The underlying physical infrastructure and th

What does this mean to me as a PCI

Our PCI Service Provider status means that customer
cardholder data can rely on our PCI compliance validat
own compliance and certification, including PCI audits a
covers all requirements as defined by PCI DSS for physi
cardholder environment to AWS can simplify your own PC
status. If your QSA currently needs additional supporting

What does this mean to me as a non-PCI

A Rackspace White Paper - Sp

Summary

Google

Search Google Checkou

< Google Checkout Merchant

Help hom

Compliance with

Google Checkout overview

Google has been certified

For more information, pleas

About Google Checkout

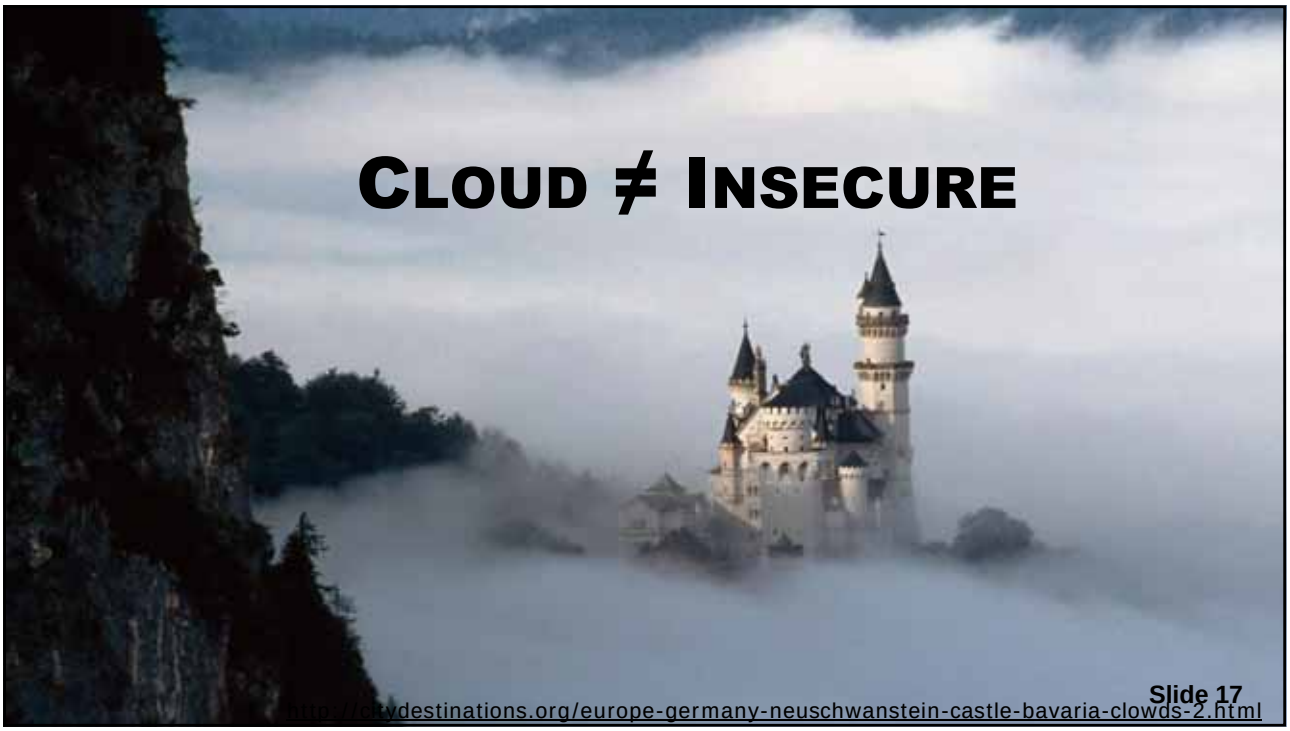
How Google Checkout works for your business

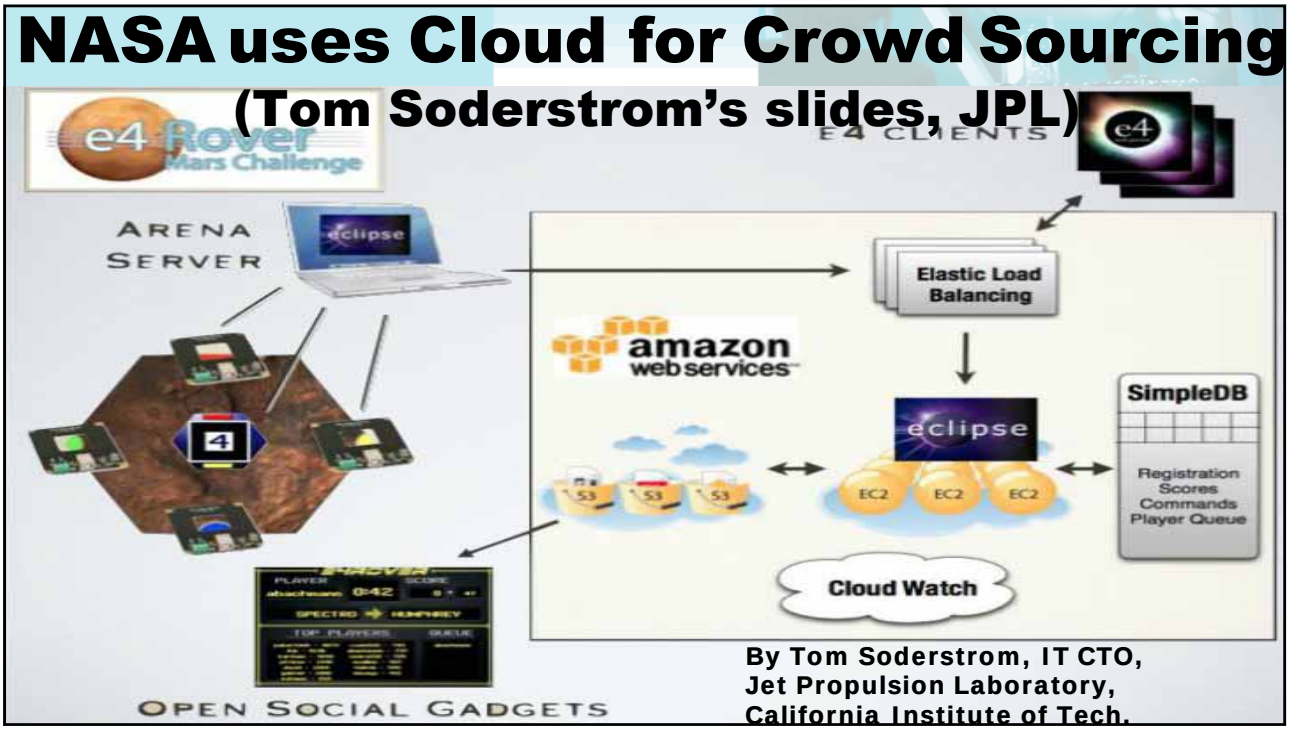
The Google Wallet buyer experience

Tell us how we're doi

Google Wallet acceptance logo

Compliance with Payment Card Industry (PCI) standards


CLOUD ≠ INSECURE
Slide 17
http://citydestinations.org/europe-germany-neuschwanstein-castle-bavaria-clowds-2.html


NASA uses Cloud for Crowd Sourcing
(Tom Soderstrom's slides, JPL)
e4 Rover Mars Challenge
E4 CLIENTS
ARENA SERVER
eclipse
Elastic Load Balancing
amazon web services
SimpleDB
eclipse
S3
EC2
Registration
Scores
Commands
Player Queue
Cloud Watch
OPEN SOCIAL GADGETS
By Tom Soderstrom, IT CTO,
Jet Propulsion Laboratory,
California Institute of Tech.

Many willingly be part of the Matrix

PCI recognises Cloud

- But **NOT** in the PCI DSS (Data Security Standard)
- "cloud" does not appear in the 75 pages of the DSS
- "virtualisation" appears **twice**:
  - "System components" includes virtualisation components such as VMs, virtual switches/routers, VAs, VSAs/SVAs, virtual applications, VDI, and hypervisors; and
  - Requirement 2.2.1: Implement only one primary function per virtual system component.

UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 20

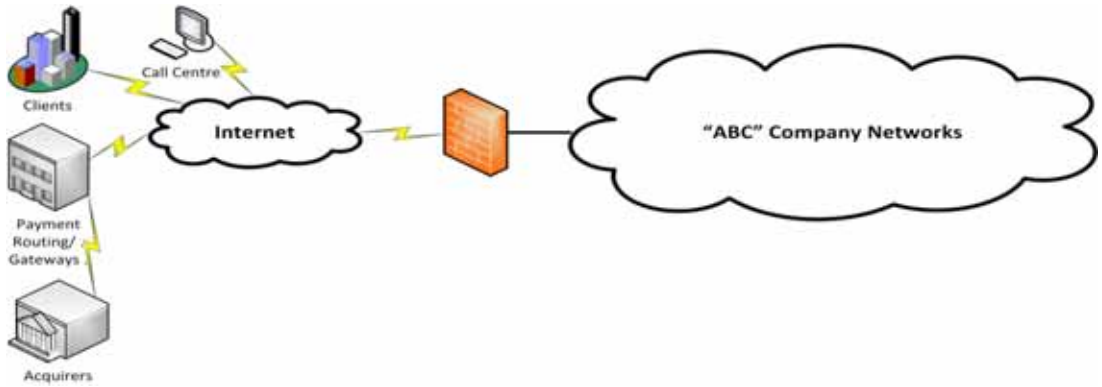
PCI DSS Virtualization Guidelines

- Virtualization Special Interest Group (SIG)
- June 2011
  PCI DSS v2.0 Information Supplement:
  PCI DSS Virtualization Guidelines

	Type of Cloud Service		
Area of Responsibility	IAAS	PAAS	SAA
Data			
Software, user applications			
Operating systems, databases			
Virtual infrastructure (hypervisor, virtual appliances, VMs, virtual networks etc)			
Computer and network hardware (processor, memory, storage, cabling, etc.)			
Data center (physical facility)			

Let's start with a reference example

- (A "real") company "ABC" 's network connections:

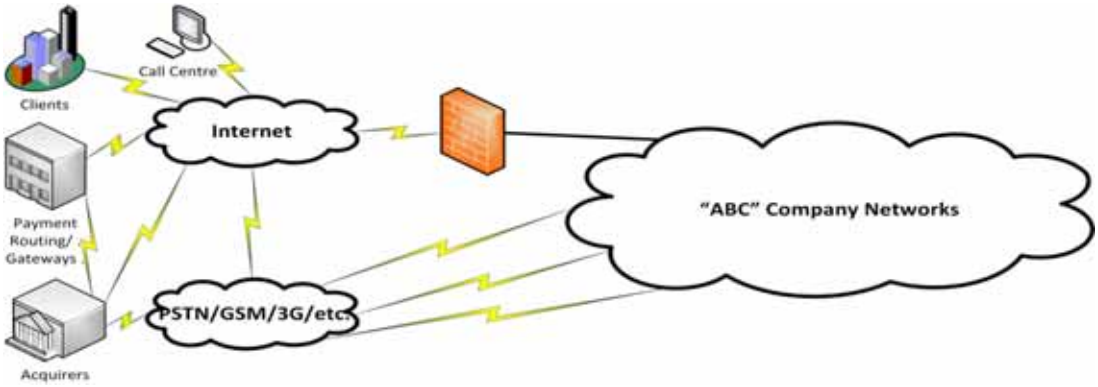


BRIDGE POINT "SECURE NETWORKING"

Slide 22

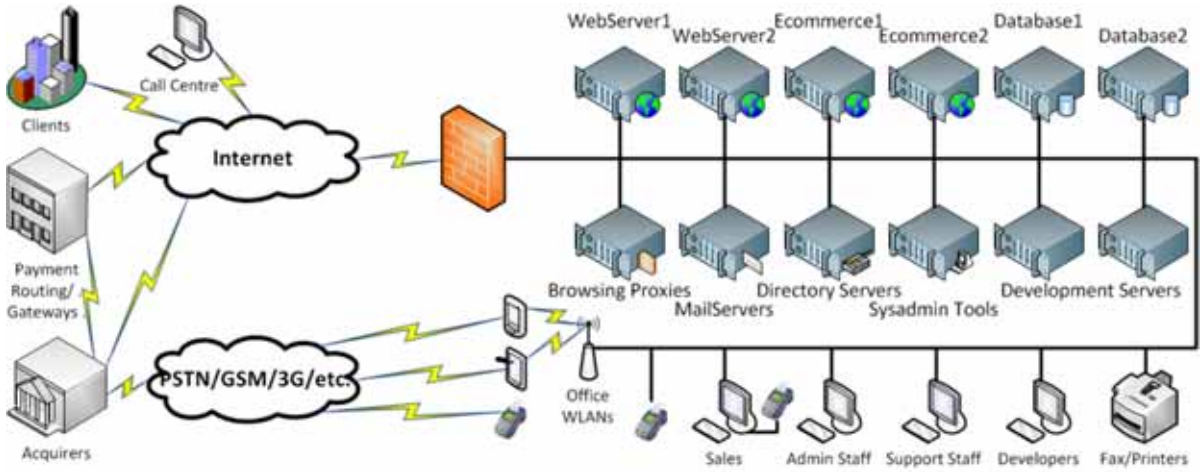
PCI is more than just "IP" security

- "ABC's" real network connections :



BRIDGE POINT "SECURE NETWORKING"

Company "ABC" pre-PCI-Compliance



BRIDGE POINT "SECURE NETWORKING"

Scope of Assessment

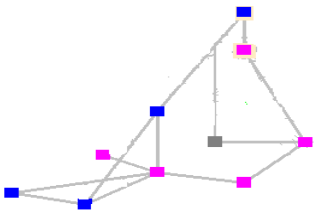
- The **cardholder data environment** is comprised of **people**, **processes**, **facilities** and **technology**, that **store**, **process**, **or transmit** cardholder data.
- PCI DSS applies to all system components
- "system components" is any network component, server, or app that is included in **or connected to** CDE
- includes **virtualisation** components such as VMs, VAs, VSAs, Vswitches/routers, VDI, **hypervisors & consoles**

UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 25

Scope – not many POS terminals

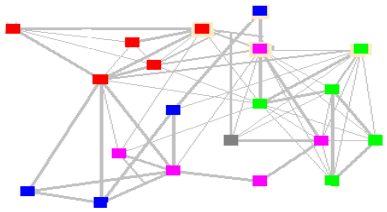


UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 26

Scope – plus hosts & printers

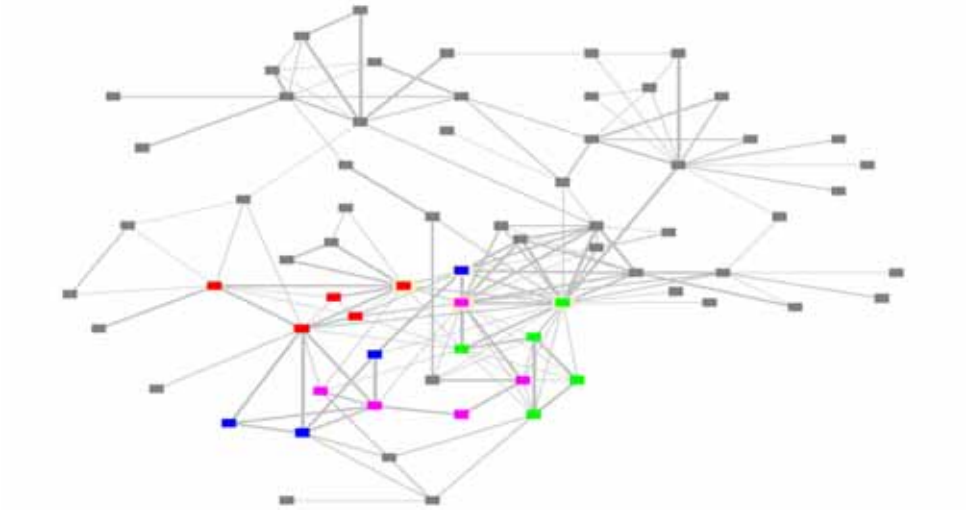


UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 27

Scope – plus supporting services

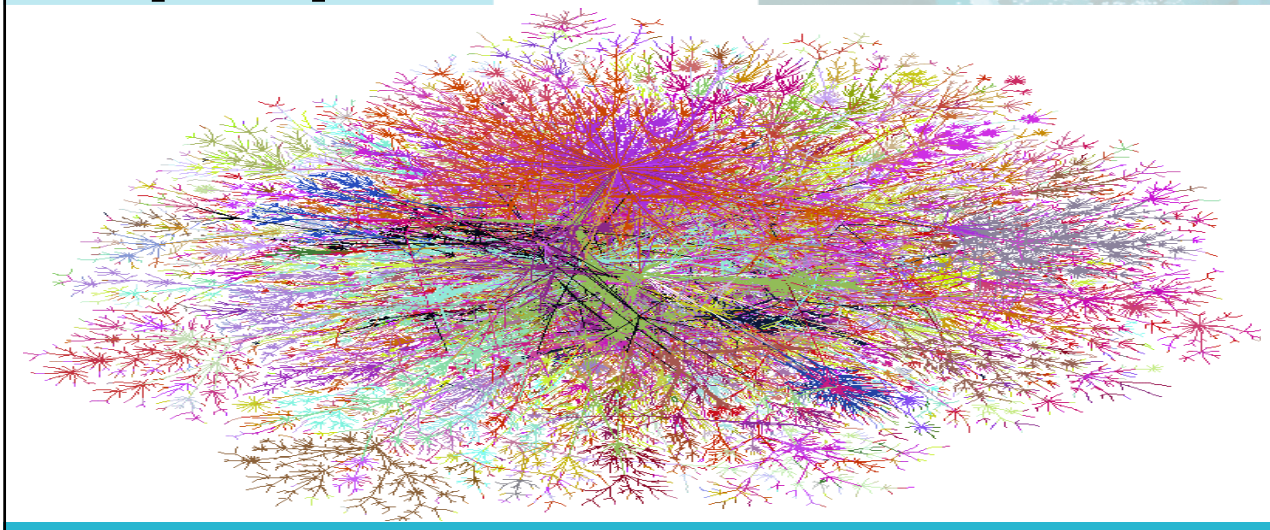


UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 28

Scope – plus ANY connected subnet



UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 29

PCI DSS is a prescriptive standard

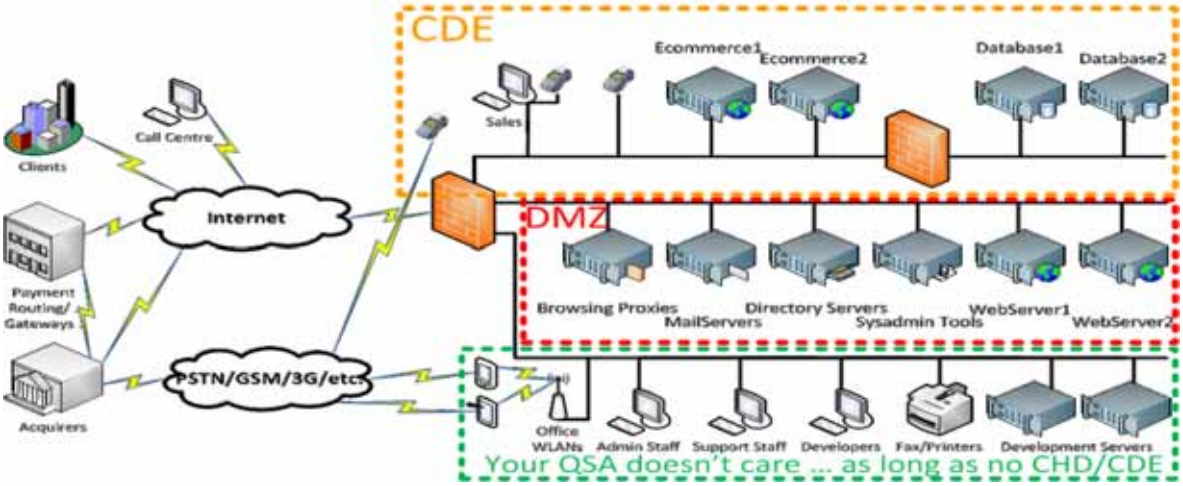
- **1.1.3** Require a firewall at each Internet connection and between any DMZ and the internal network zone
- **1.2.3** Install perimeter firewalls between any wireless networks and the cardholder data environment
- **1.3.2** Limit inbound Internet traffic to IPaddr within DMZ
- **1.3.3** Do not allow direct connections inbound or outbou
- **1.3.7** Place components that store CHD (files or DBs) in an internal network segregated from DMZs

UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 30

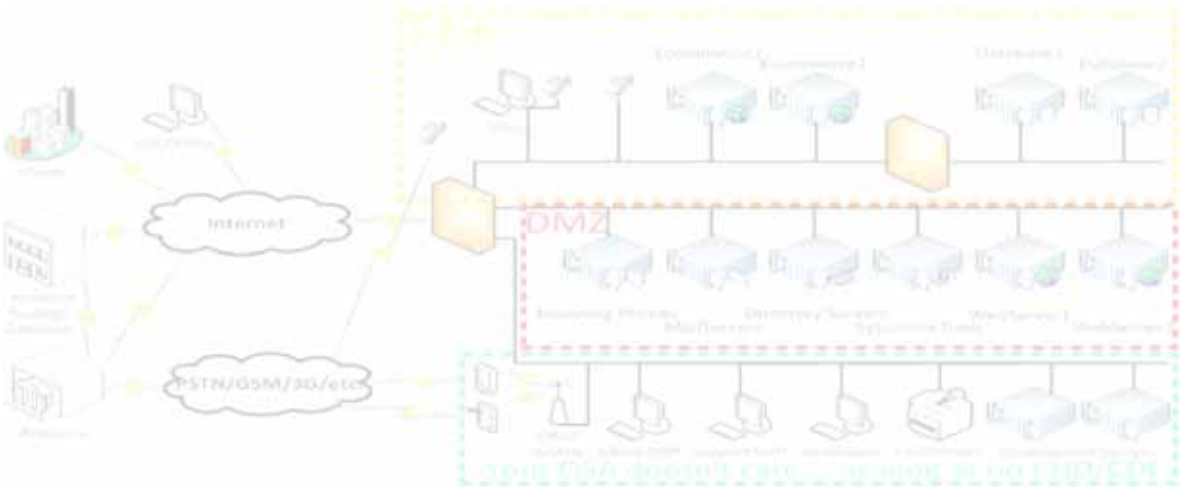
"ABC" Post-PCI (two years ago):



BRIDGE POINT "SECURE NETWORKING"

Slide 31

Then they went virtual...



BRIDGE POINT "SECURE NETWORKING"

Slide 32

Many QSAs declared virtualised environments non-compliant

- **1.3.7** Place systems store CHD segregated from DMZs
- **2.2.1** Implement only one primary function per server
- **2.4** Hosting providers must prot each entity's env & CHD
- **6.4.1** Separate development/test and production env's
- **11.4** Use IDS or IPS to monitor ALL traffic at the perimeter of the CDE **as well as at critical points inside**

UNCLASSIFIED

Slide 33

Cloud was even harder…

- All the above plus more
- **5.2** Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs
- **6.1** Install critical patches within one month of release
- **6.4.5.4** Back-out procedures in change control
- **6.6** Public-facing web applications: annual application vulnerability security assessment or install a WAF
- **7.1&7.2** Limit access to systems: RBAC & need-to-know

UNCLASSIFIED

Slide 34

And public cloud had no chance...

- **9.1.3** Restrict physical access to gateways, devices, networking/communications hardware, and telecomms
- **10.2** Implement automated audit trails for all components
- **11.2** Run internal & external vulnerability scans quarterly
- **11.3** Perform external & internal pen testing annually
- **11.5** Deploy file-integrity monitoring for critical system files, configuration files, and content files

UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 35

If virtualisation is implemented,

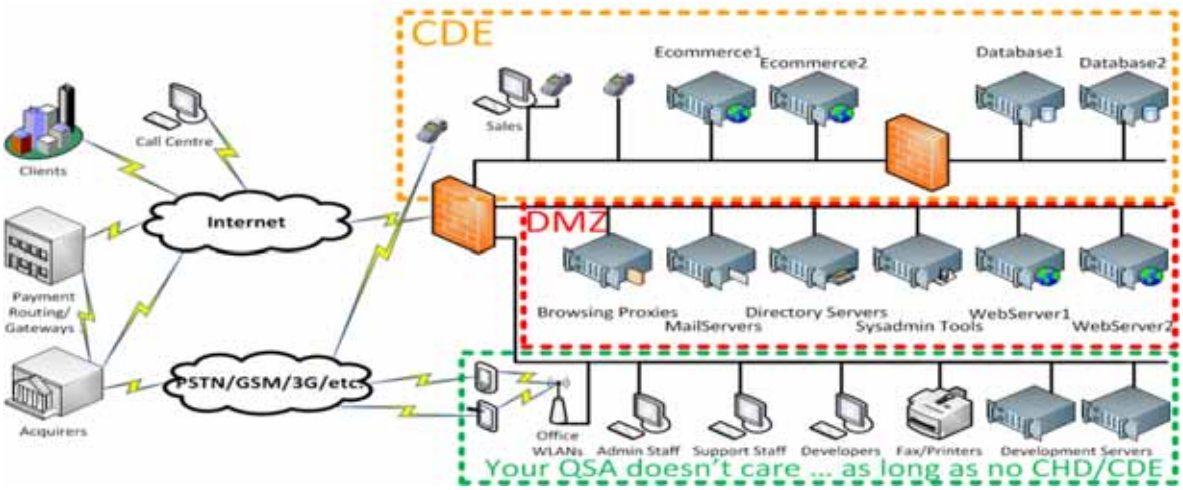
- All components within the virtual environment will need to be identified and considered in scope
  - including individual virtual hosts or devices,
  - management interfaces,
  - central management consoles,
  - hypervisors, and
  - all intra-host and external communications and data flows.

UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 36

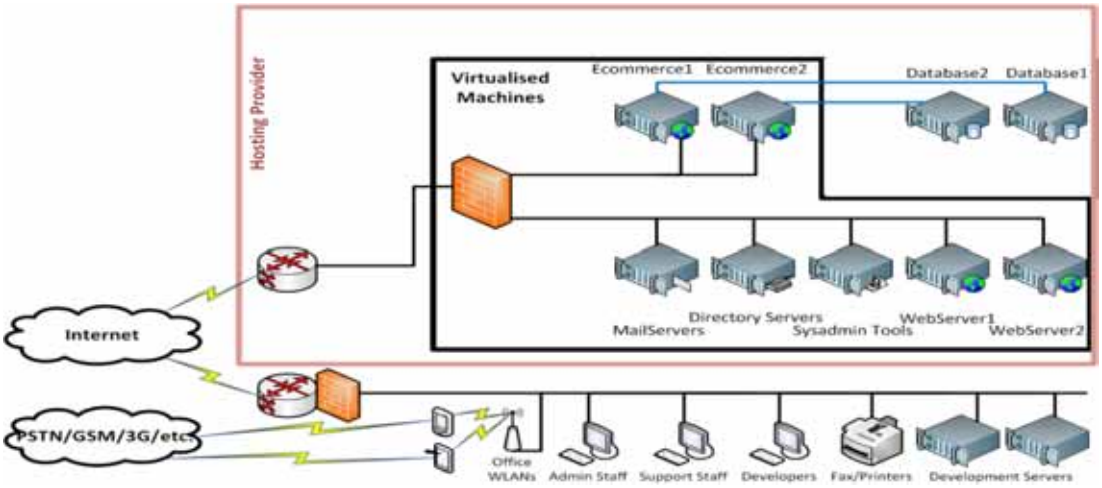
"ABC" Post-PCI Pre-virtual CDE:



BRIDGE POINT "SECURE NETWORKING"

Slide 37

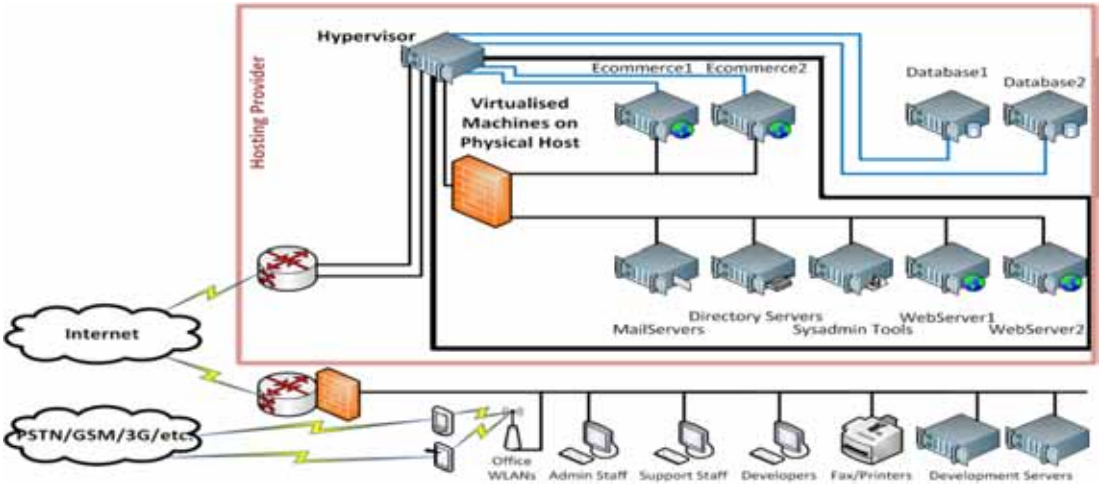
How the Sysadmin Saw It:



BRIDGE POINT "SECURE NETWORKING"

Slide 38

How the Auditor Saw It:



BRIDGE POINT "SECURE NETWORKING"

Slide 39

Your hypervisor is NOT a firewall

- A virtual firewall (VM or VSA/SVA) is fine
- It can segment your virtual networks including your CDE
- It can **NOT** protect the hypervisor it is running on
- A hypervisor running *any* CDE guest is automatically CDE
- No part of CDE may directly connect to untrusted netwrk
- A hypervisor running *any* CDE guest VM or VA can **NOT** be directly connected to untrusted networks

BRIDGE POINT "SECURE NETWORKING"

Slide 40

Hypervisor attack surface

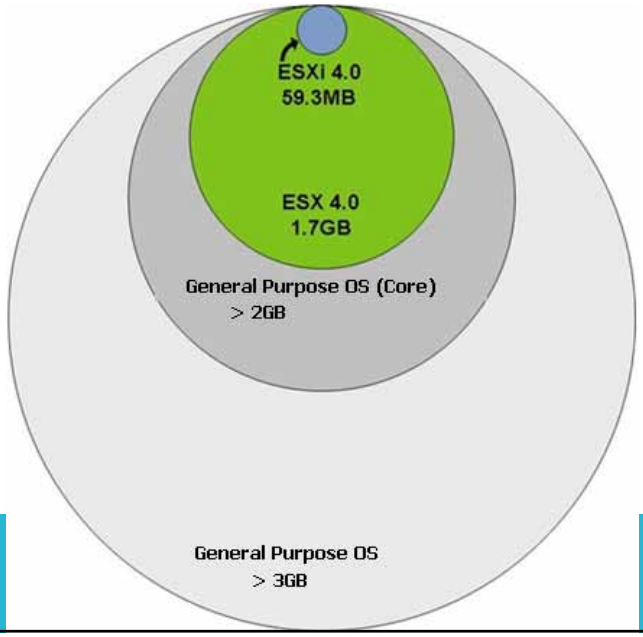
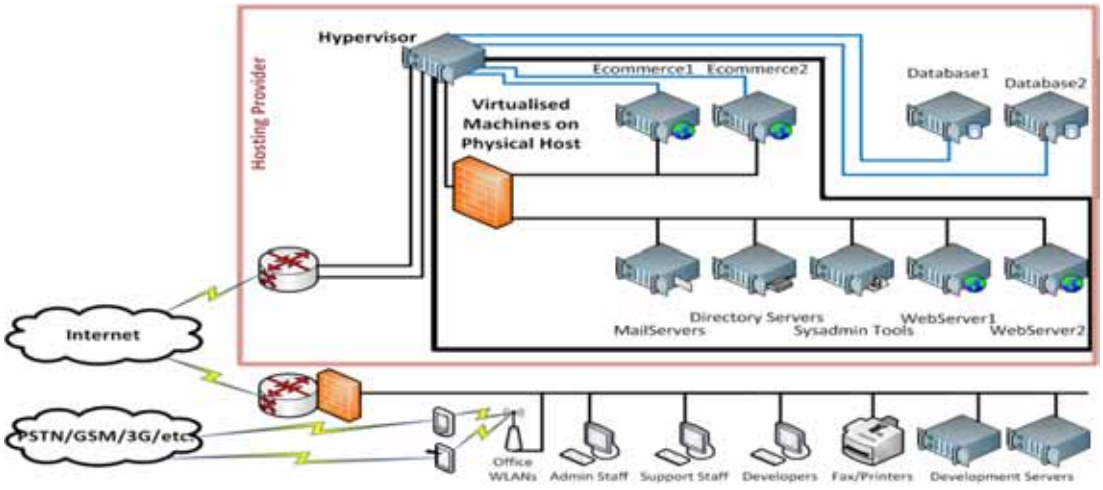


Image Source:
VMware (EMC)
marketing material

PUBLIC

Slide 41

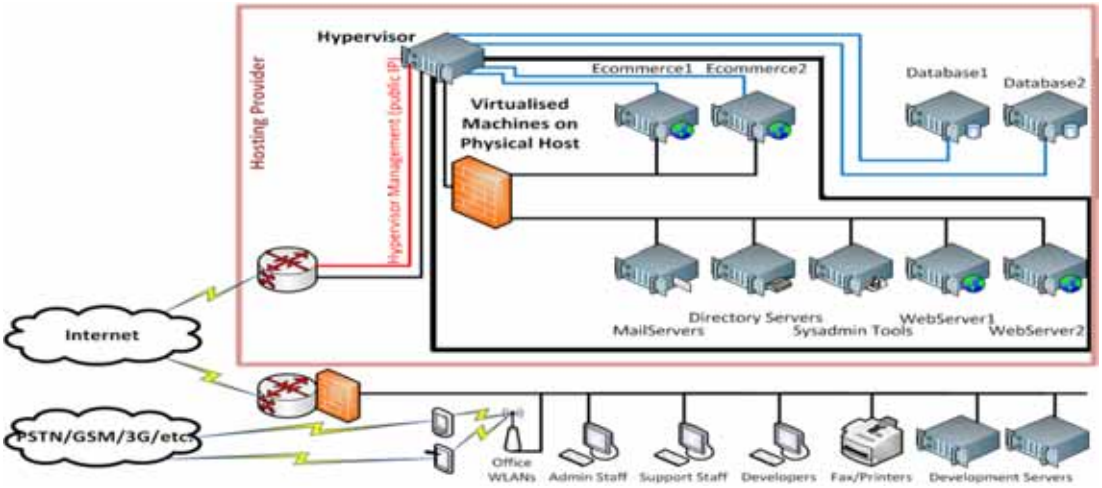
Back to our example:



BRIDGE POINT
"SECURE NETWORKING"

Slide 42

And the Final Kicker:



BRIDGE POINT "SECURE NETWORKING"

Slide 43

VSIG: Mixed-Mode Environments

- Strongly recommended (and a basic security principle)
  - VMs of different security levels **are not hosted on the same hypervisor or physical host**
  - concern VM with lower security could launch attack on others
- This should also be applied if in-scope & out-of-scope virtual systems located on the same host or hypervisor.

UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 44

PCI VSIG Cloud killer:

- **General rule: any VM or other virtual component that is hosted on same hardware or hypervisor as an in-scope component would also be in scope for PCI DSS**,

  as both the hypervisor & underlying host provide a connection (either physical, logical, or both)

VSIG Cloud Computing "catch-all"

- **Entities planning to use cloud computing for PCI should first ensure they thoroughly understand the details of the services offered, & perform a detailed assessment of the unique risks with each service.**
- **…it is crucial that the hosted entity and provider clearly document the responsibilities assigned to each party for maintaining PCI DSS requirements and controls that could impact the security of CHD.**

NIST
Cloud Computing
Reference Architecture

Version 1

March 30, 2011

Information Technology Laboratory Cloud Computing Program

NIST National Institute of Standards and Technology U.S. Department of Commerce

Three Cloud Service Models

- Cloud Software as a Service (SaaS)
- Cloud Platform as a Service (PaaS)
- Cloud Infrastructure as a Service (IaaS)

Four Cloud Deployment Models

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 49

PCI's version of Private Cloud

- System components trusted & controlled by the entity
- Owned by the entity or a third party
- In facilities owned by the entity or a third party
  - May be owned by a service provider and provisioned for dedicated use by a single customer
- Irrespective of ownership, dedicated to a single entity and are not shared with any other customer or tenant

UNCLASSIFIED

BRIDGE POINT "SECURE NETWORKING"

Slide 50

PCI's version of Public Cloud

- Service-based access for multiple customers or tenants, to shared computing resources, the entity does not own or have control over
- Components remaining under control of provider will vary according to type of service — IaaS, PaaS, SaaS
- Physical separation between tenants is not practical — by its very nature, resources are shared by everyone

UNCLASSIFIED

Slide 51

PCI's version of Hybrid Cloud

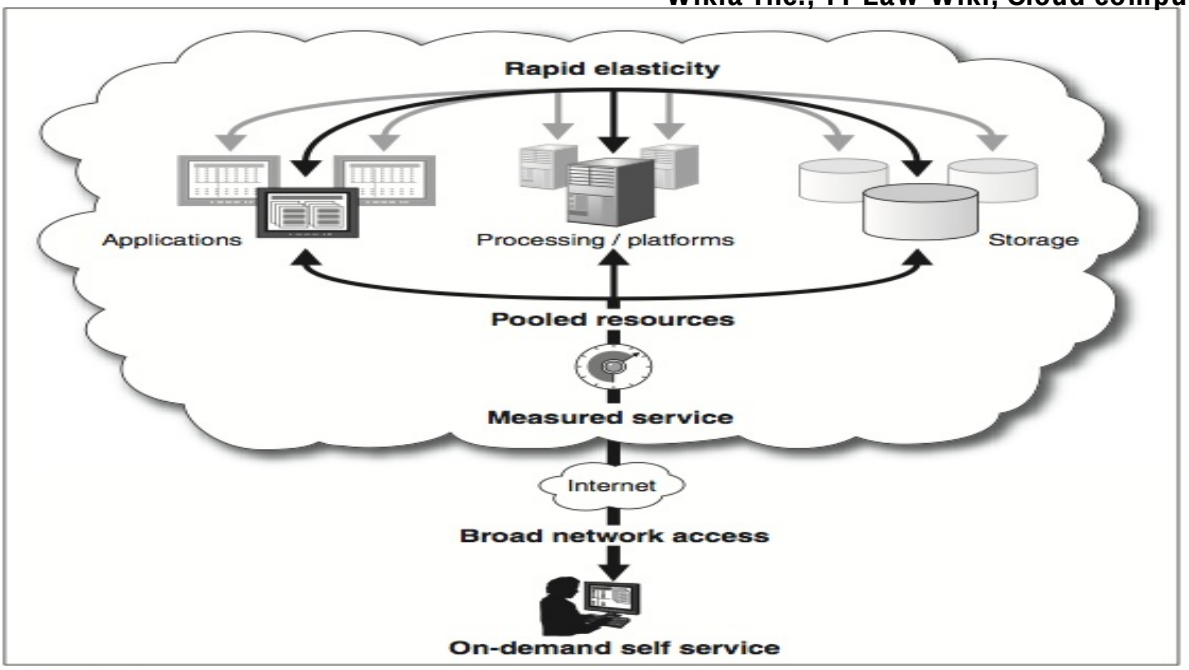
- Combination of private & public cloud infrastructures
- Public cloud or another entity's private cloud
- Ownership & control of data and system components may be divided b/w three or more separate entities
- Complex scope boundaries & defining responsibilities

UNCLASSIFIED

Slide 52

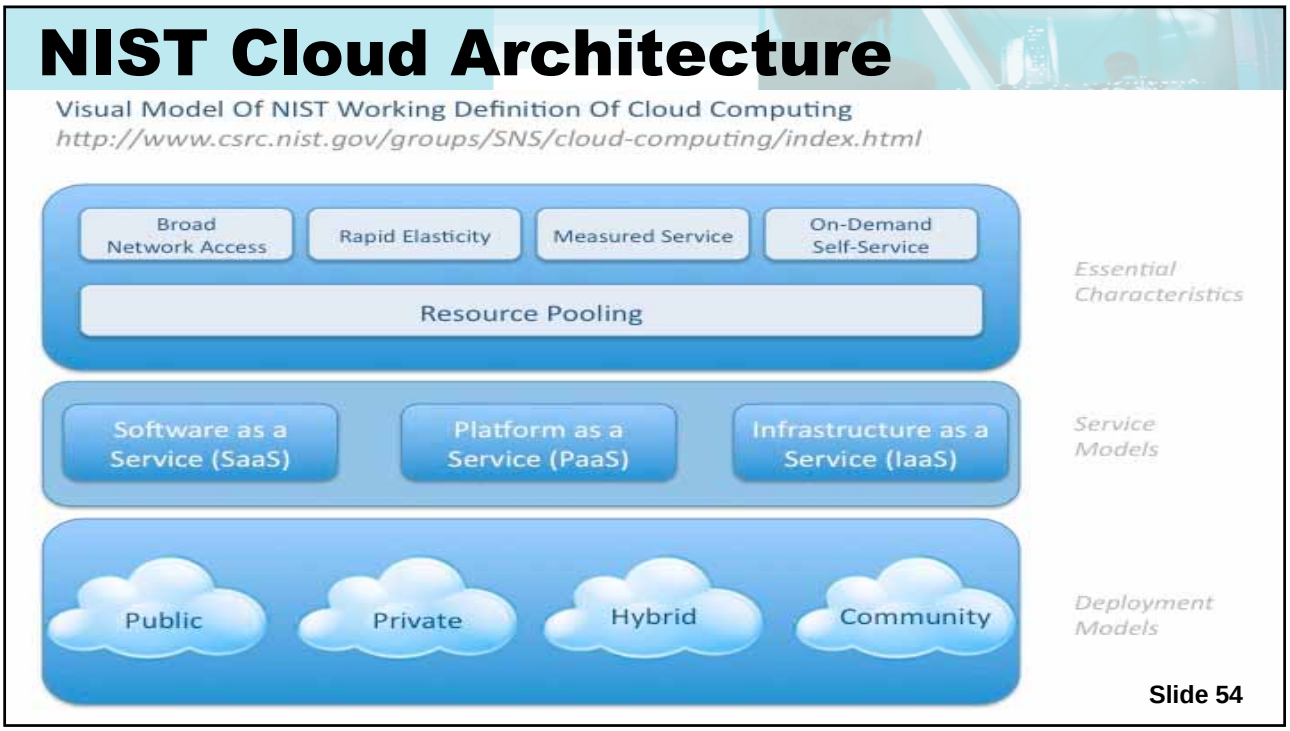
Figure 3: NIST Essential Characteristics

Wikia Inc., IT Law Wiki, Cloud computing



Source: GAO.

http://images.wikia.com/itlaw/images/7/7f/Cloud5.jpg



Cloud Security Alliance

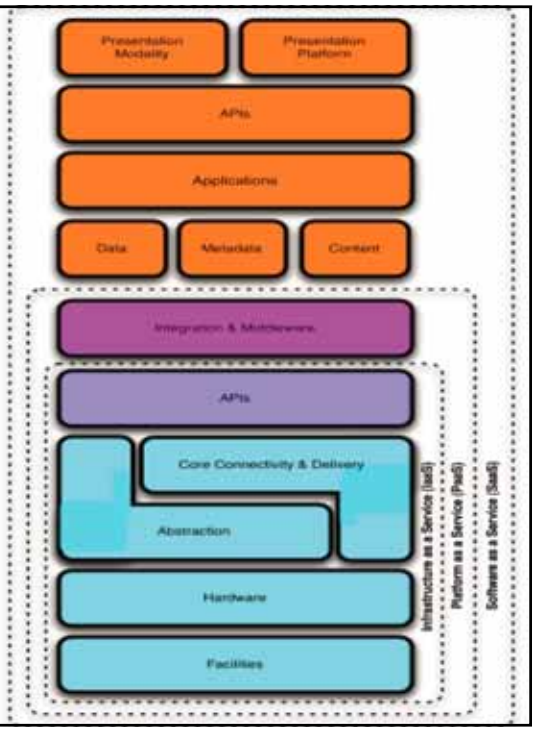
SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0

CSA Australia meeting 12:35 THU

Reference Model

- Cloud Software as a Service (SaaS)
- Cloud Platform as a Service (PaaS)
- Cloud Infrastructure as a Service (IaaS)

Image Source: Cloud Security Alliance Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, p.18



Moving to The Cloud…

NASA – *Space Shuttle Rising* (May 2011)

1. Have Someone Else Do It

2. Non-PCI Cloud Offerings

- Use public cloud (SaaS, PaaS, IaaS)
- Cloud environment segmented from CDE
- NO PANs in any cloud environment
- Truncation / Hashing / Tokenisation
- NO encrypted PANs! … well maybe …

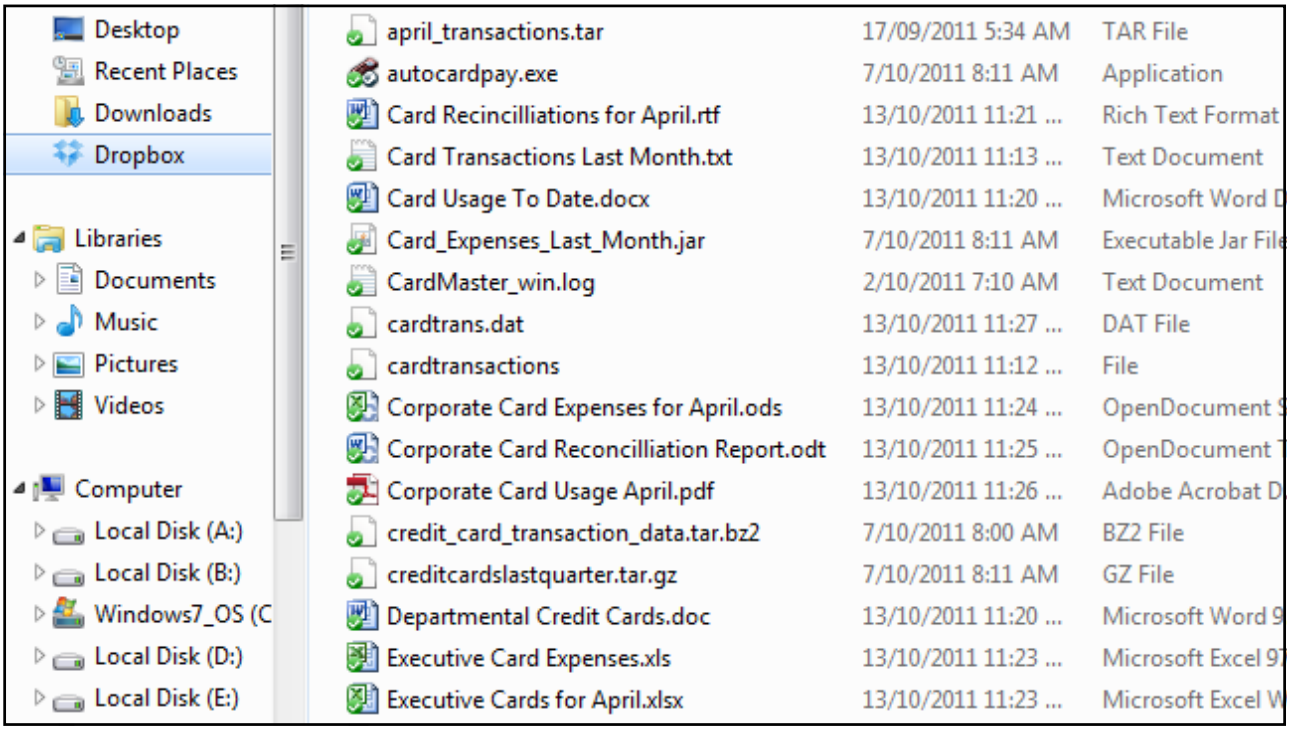
BRIDGE POINT "SECURE NETWORKING"

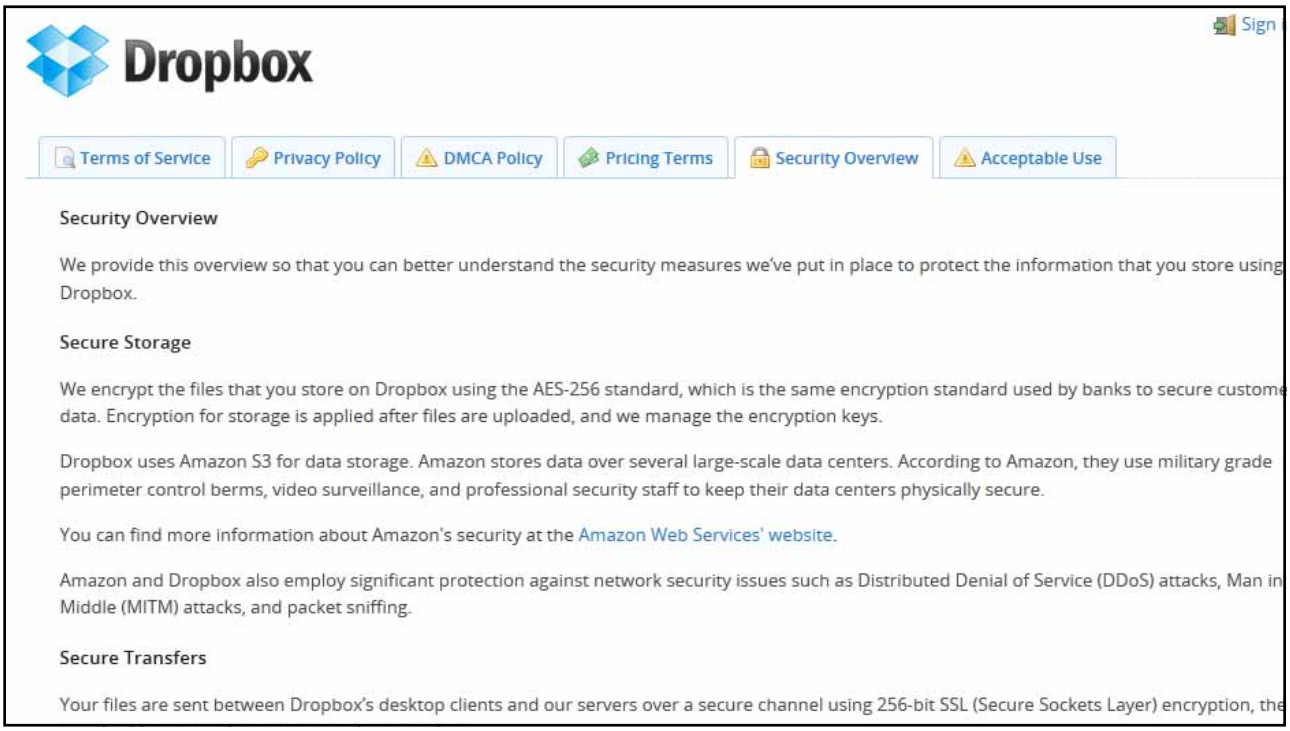
Common PAN Leakage

- Excel spreadsheet on cloud systems
  - Box, Dropbox, Google Documents
- Application screenshots
- Finance and HR documents with PANs
- Other Office formats with PAN information
- Text dumps from poorly-written/legacy applications

BRIDGE POINT "SECURE NETWORKING"

Slide 61





Dropbox

Terms of Service | Privacy Policy | DMCA Policy | Pricing Terms | Security Overview | Acceptable Use

Security Overview

We provide this overview so that you can better understand the security measures we've put in place to protect the information that you store using Dropbox.

Secure Storage

We encrypt the files that you store on Dropbox using the AES-256 standard, which is the same encryption standard used by banks to secure custome data. Encryption for storage is applied after files are uploaded, and we manage the encryption keys.

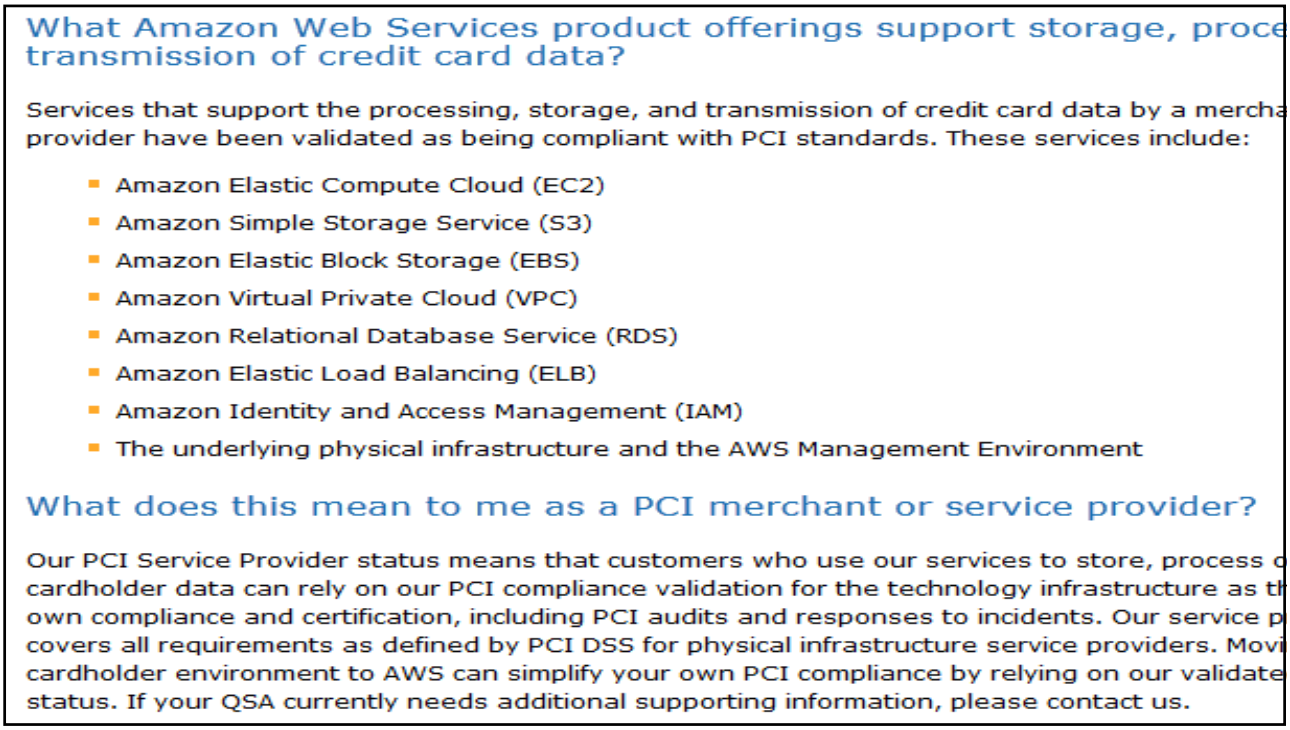
Dropbox uses Amazon S3 for data storage. Amazon stores data over several large-scale data centers. According to Amazon, they use military grade perimeter control berms, video surveillance, and professional security staff to keep their data centers physically secure.

You can find more information about Amazon's security at the Amazon Web Services' website.

Amazon and Dropbox also employ significant protection against network security issues such as Distributed Denial of Service (DDoS) attacks, Man in Middle (MITM) attacks, and packet sniffing.

Secure Transfers

Your files are sent between Dropbox's desktop clients and our servers over a secure channel using 256-bit SSL (Secure Sockets Layer) encryption, the



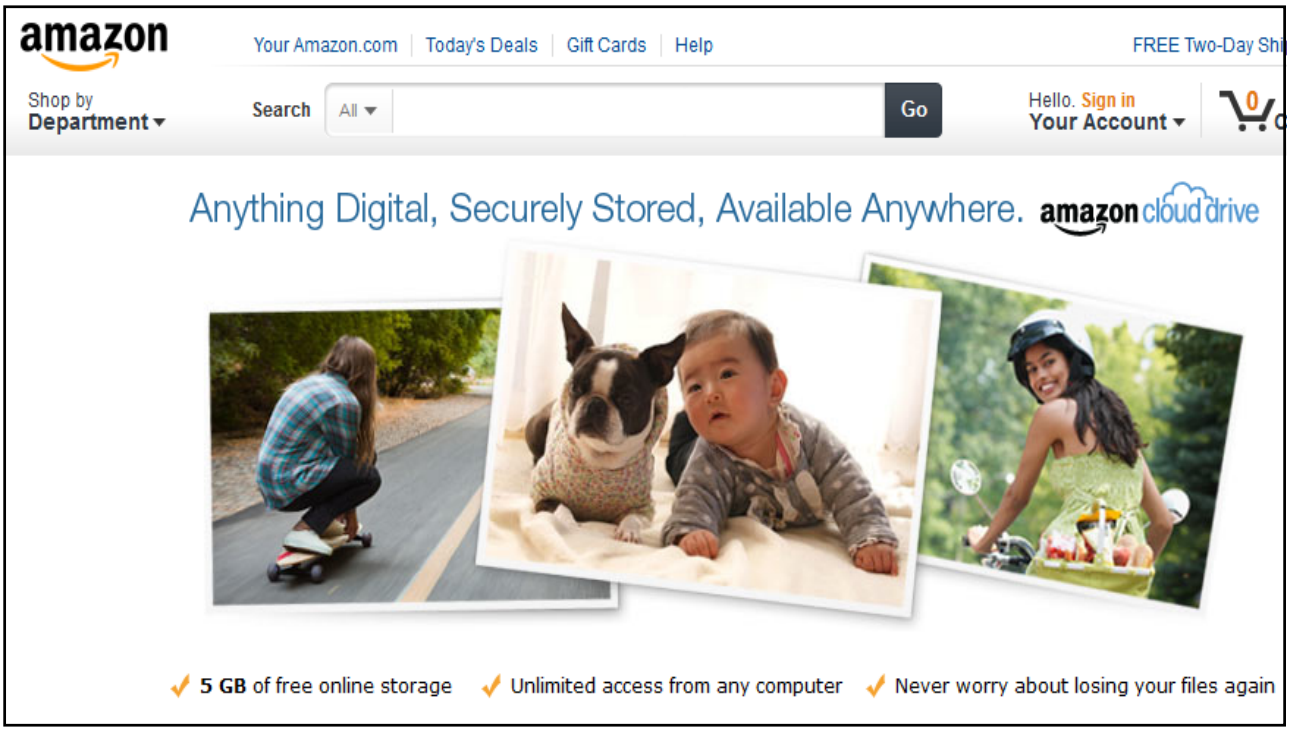
What Amazon Web Services product offerings support storage, proce transmission of credit card data?

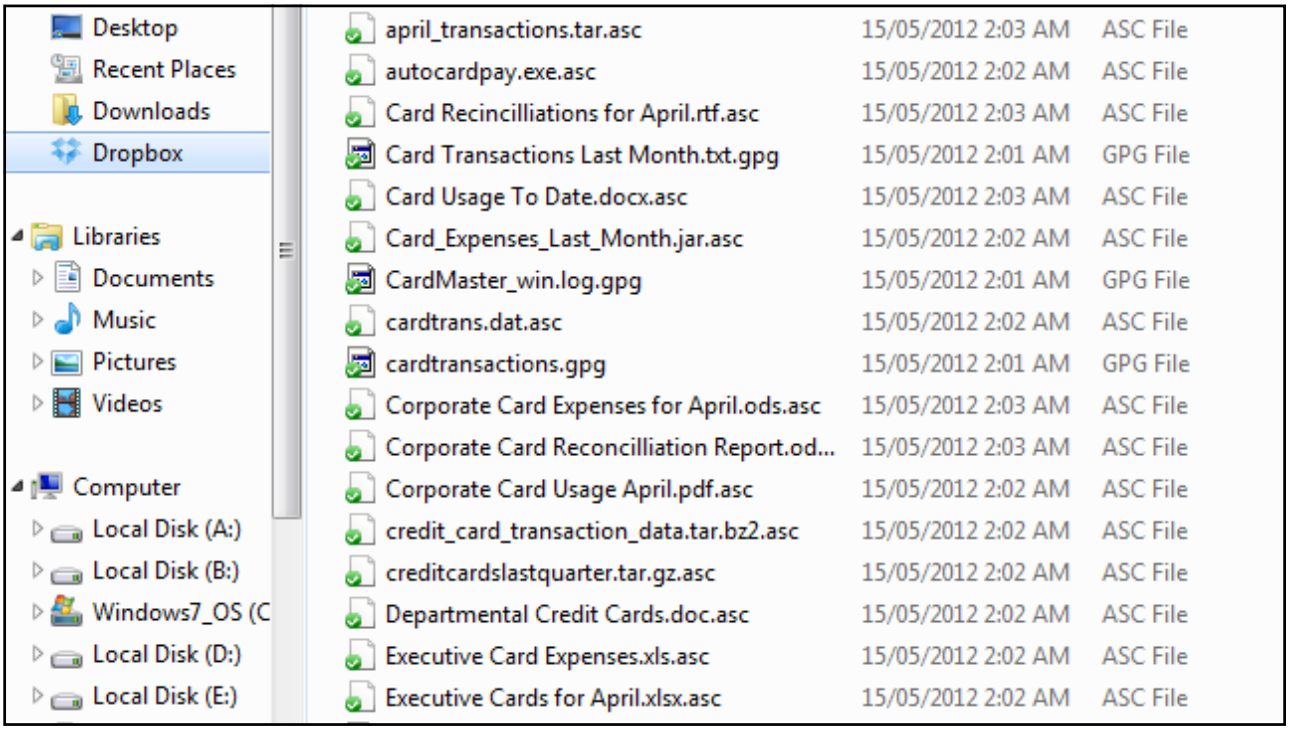
Services that support the processing, storage, and transmission of credit card data by a mercha provider have been validated as being compliant with PCI standards. These services include:

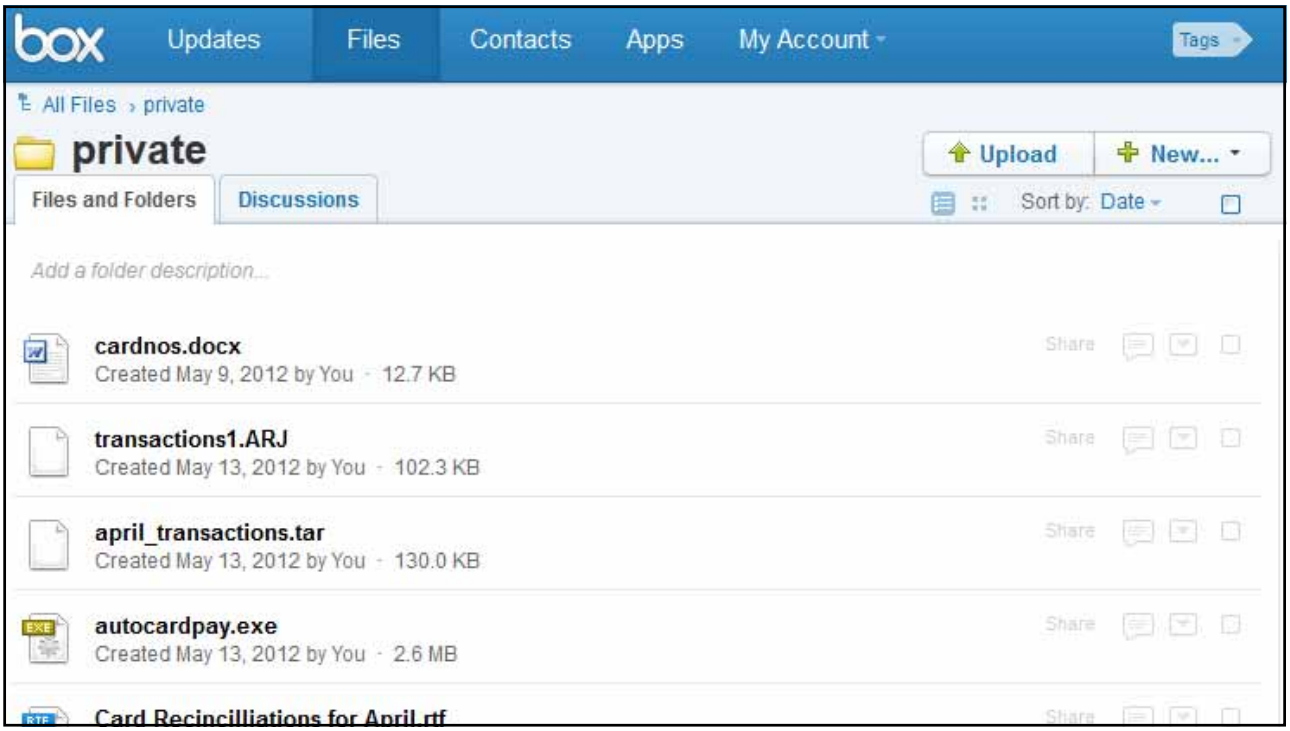
- Amazon Elastic Compute Cloud (EC2)
- Amazon Simple Storage Service (S3)
- Amazon Elastic Block Storage (EBS)
- Amazon Virtual Private Cloud (VPC)
- Amazon Relational Database Service (RDS)
- Amazon Elastic Load Balancing (ELB)
- Amazon Identity and Access Management (IAM)
- The underlying physical infrastructure and the AWS Management Environment

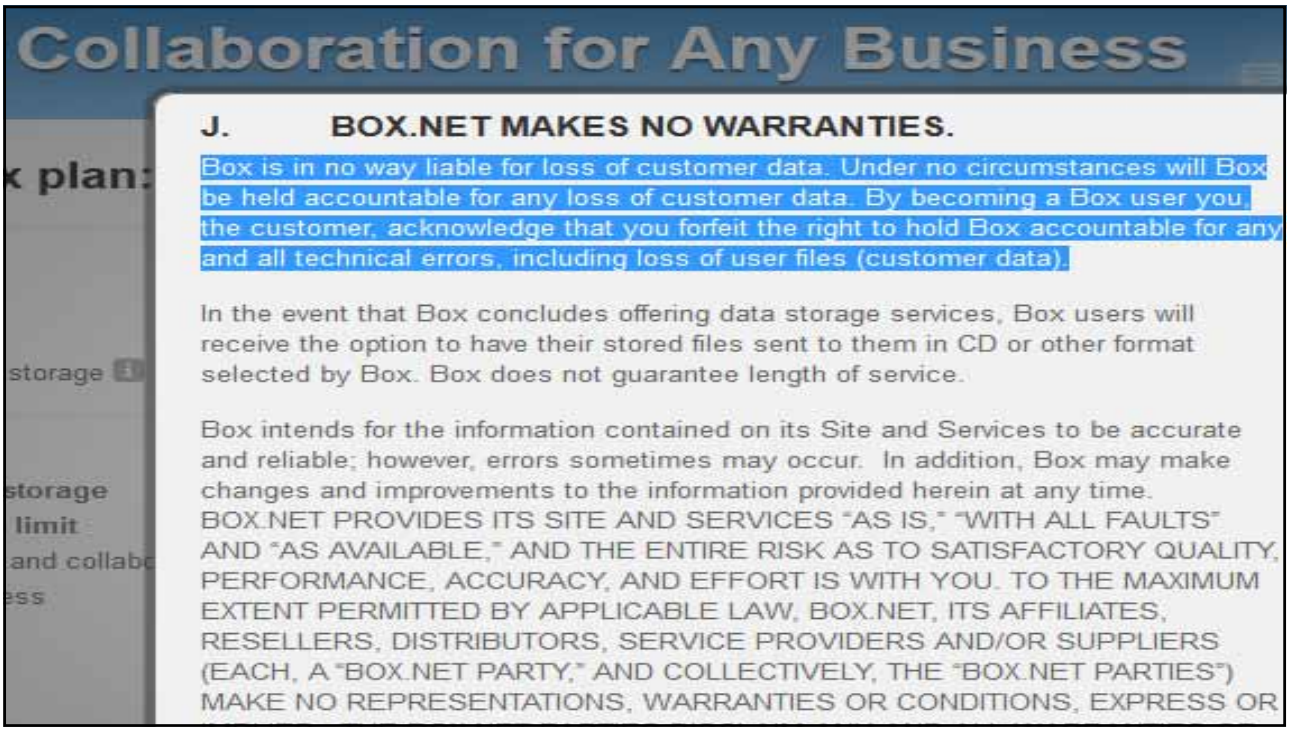
What does this mean to me as a PCI merchant or service provider?

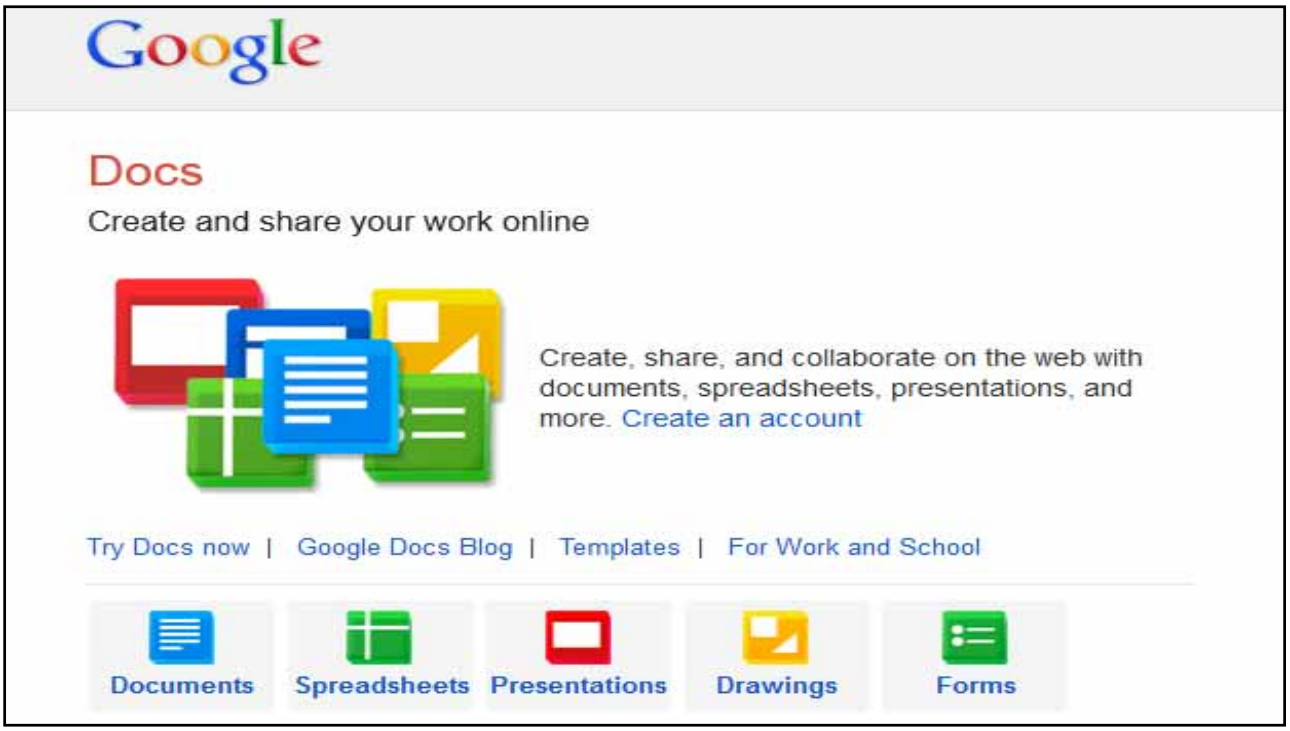
Our PCI Service Provider status means that customers who use our services to store, process o cardholder data can rely on our PCI compliance validation for the technology infrastructure as th own compliance and certification, including PCI audits and responses to incidents. Our service p covers all requirements as defined by PCI DSS for physical infrastructure service providers. Movi cardholder environment to AWS can simplify your own PCI compliance by relying on our validate status. If your QSA currently needs additional supporting information, please contact us.

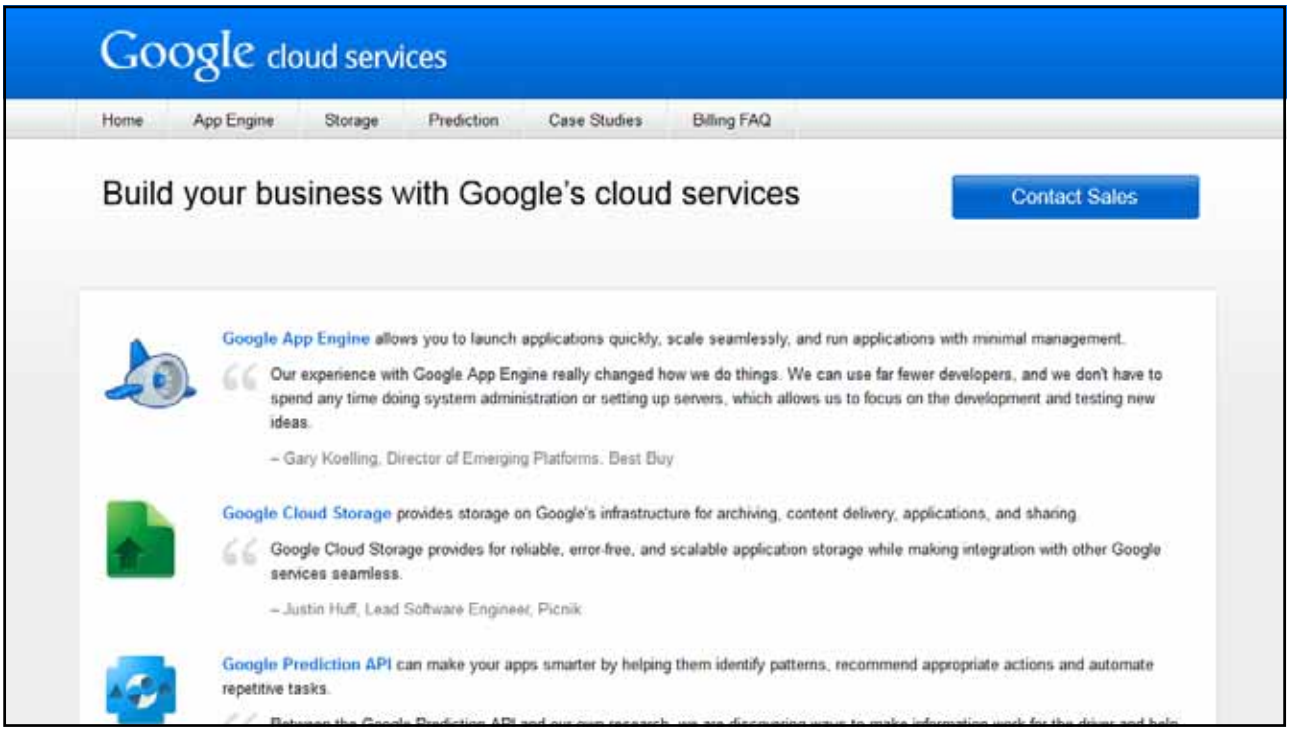

amazon
Your Amazon.com
Today's Deals
Gift Cards
Help
FREE Two-Day Shi
Shop by Department
Search
All
Go
Hello. Sign in
Your Account
Anything Digital, Securely Stored, Available Anywhere.
amazon cloud drive
5 GB of free online storage
Unlimited access from any computer
Never worry about losing your files again


Desktop
Recent Places
Downloads
Dropbox
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (A:)
Local Disk (B:)
Windows7_OS (C
Local Disk (D:)
Local Disk (E:)
april_transactions.tar.asc 15/05/2012 2:03 AM ASC File
autocardpay.exe.asc 15/05/2012 2:02 AM ASC File
Card Recincilliations for April.rtf.asc 15/05/2012 2:03 AM ASC File
Card Transactions Last Month.txt.gpg 15/05/2012 2:01 AM GPG File
Card Usage To Date.docx.asc 15/05/2012 2:03 AM ASC File
Card_Expenses_Last_Month.jar.asc 15/05/2012 2:02 AM ASC File
CardMaster_win.log.gpg 15/05/2012 2:01 AM GPG File
cardtrans.dat.asc 15/05/2012 2:02 AM ASC File
cardtransactions.gpg 15/05/2012 2:01 AM GPG File
Corporate Card Expenses for April.ods.asc 15/05/2012 2:03 AM ASC File
Corporate Card Reconcilliation Report.od... 15/05/2012 2:03 AM ASC File
Corporate Card Usage April.pdf.asc 15/05/2012 2:02 AM ASC File
credit_card_transaction_data.tar.bz2.asc 15/05/2012 2:02 AM ASC File
creditcardslastquarter.tar.gz.asc 15/05/2012 2:02 AM ASC File
Departmental Credit Cards.doc.asc 15/05/2012 2:02 AM ASC File
Executive Card Expenses.xls.asc 15/05/2012 2:02 AM ASC File
Executive Cards for April.xlsx.asc 15/05/2012 2:02 AM ASC File


box
Updates
Files
Contacts
Apps
My Account
Tags
All Files › private
private
Upload
New...
Files and Folders
Discussions
Sort by: Date
Add a folder description...
cardnos.docx
Created May 9, 2012 by You · 12.7 KB
transactions1.ARJ
Created May 13, 2012 by You · 102.3 KB
april_transactions.tar
Created May 13, 2012 by You · 130.0 KB
autocardpay.exe
Created May 13, 2012 by You · 2.6 MB
Share


Collaboration for Any Business
J. BOX.NET MAKES NO WARRANTIES.
Box is in no way liable for loss of customer data. Under no circumstances will Box be held accountable for any loss of customer data. By becoming a Box user you, the customer, acknowledge that you forfeit the right to hold Box accountable for any and all technical errors, including loss of user files (customer data).
In the event that Box concludes offering data storage services, Box users will receive the option to have their stored files sent to them in CD or other format selected by Box. Box does not guarantee length of service.
Box intends for the information contained on its Site and Services to be accurate and reliable; however, errors sometimes may occur. In addition, Box may make changes and improvements to the information provided herein at any time.
BOX.NET PROVIDES ITS SITE AND SERVICES "AS IS," "WITH ALL FAULTS" AND "AS AVAILABLE," AND THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY, AND EFFORT IS WITH YOU. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, BOX.NET, ITS AFFILIATES, RESELLERS, DISTRIBUTORS, SERVICE PROVIDERS AND/OR SUPPLIERS (EACH, A "BOX.NET PARTY," AND COLLECTIVELY, THE "BOX.NET PARTIES") MAKE NO REPRESENTATIONS, WARRANTIES OR CONDITIONS, EXPRESS OR

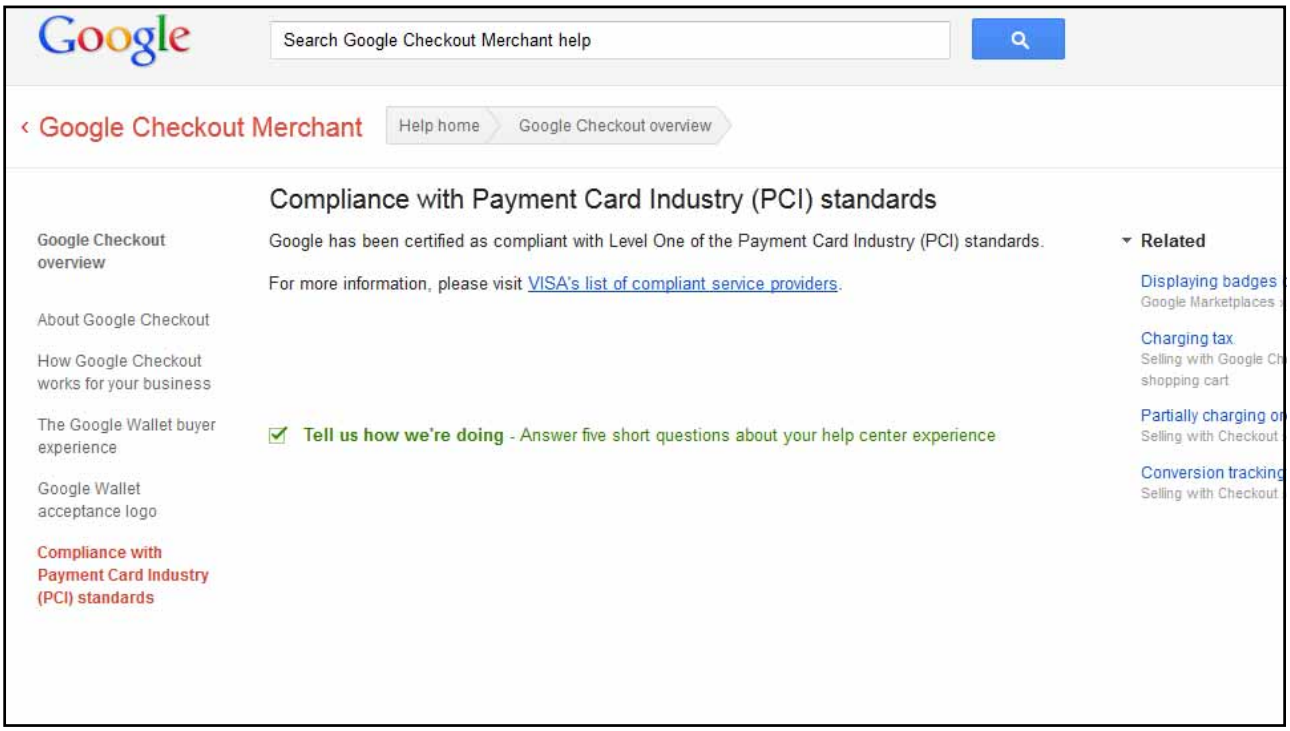

Google
Docs
Create and share your work online
Create, share, and collaborate on the web with documents, spreadsheets, presentations, and more. Create an account
Try Docs now | Google Docs Blog | Templates | For Work and School
Documents
Spreadsheets
Presentations
Drawings
Forms


Google cloud services
Home
App Engine
Storage
Prediction
Case Studies
Billing FAQ
Build your business with Google's cloud services
Contact Sales
Google App Engine allows you to launch applications quickly, scale seamlessly, and run applications with minimal management.
Our experience with Google App Engine really changed how we do things. We can use far fewer developers, and we don't have to spend any time doing system administration or setting up servers, which allows us to focus on the development and testing new ideas.
– Gary Koelling, Director of Emerging Platforms, Best Buy
Google Cloud Storage provides storage on Google's infrastructure for archiving, content delivery, applications, and sharing.
Google Cloud Storage provides for reliable, error-free, and scalable application storage while making integration with other Google services seamless.
– Justin Huff, Lead Software Engineer, Picnik
Google Prediction API can make your apps smarter by helping them identify patterns, recommend appropriate actions and automate repetitive tasks.

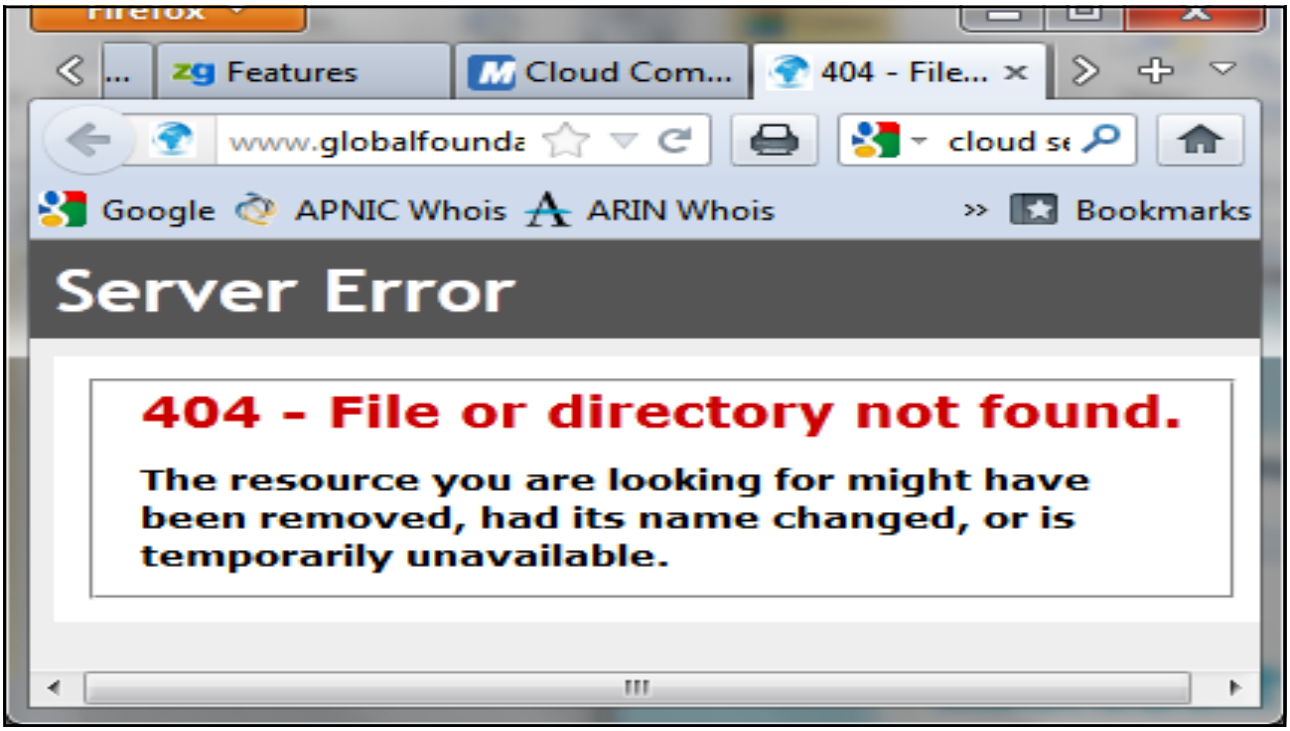
2. Provision of the Service.

2.1 Console. Google will provide the Service to Customer. As part of receiving the Service, Customer will have access to the Admin Console, through which Customer may administer the Service.

2.2 Facilities and Data Transfer. All facilities used to store and process an Application (including Customer Content) will adhere to reasonable security standards no less protective than the security standards at facilities where Google processes and stores its own information of a similar type. Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of an Application and Customer Content, protect against anticipated threats or hazards to the security or integrity of an Application and Customer Content, and protect against unauthorized access to or use of an Application and Customer Content. Google may process and store an Application and Customer Content in the United States or any other country in which Google or its agents maintain facilities. By using the Service, Customer consents to this processing and storage of the Application and Customer Content.



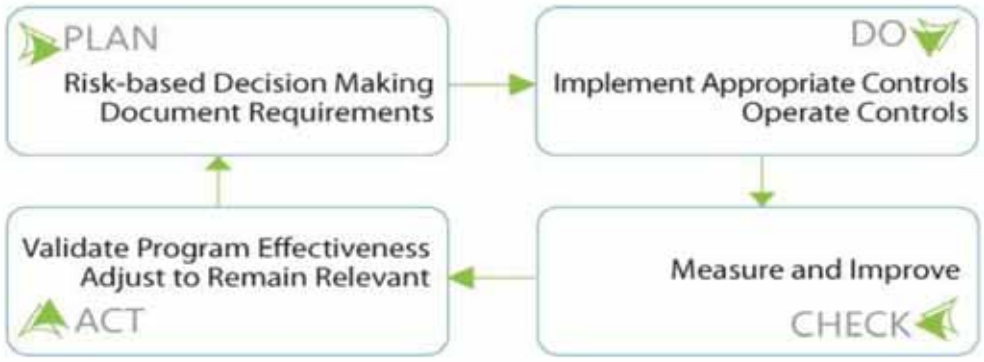

Tools & Resources
Microsoft
HOW MICROSOFT ADDRESSES THE FOUR TOP CLOUD COMPUTING ISSUES
When considering cloud computing solutions, organisations list security, privacy, reliability, and operational control as key issues.
Microsoft addresses these issues through the coordinated and strategic application of people, processes, technologies, and experience. The result is continuous cloud security advances within the Microsoft cloud environment. This provides organisations with the freedom to engage in an expansive portfolio of cloud solutions, where they can save money and refocus on their core competencies.
TAGS: cloud, cloud technologies, cloud computing, security, Microsoft
DOWNLOAD THE WHITE PAPER


Features
Cloud Com...
404 - File...
www.globalfounda
cloud se
Google
APNIC Whois
ARIN Whois
Bookmarks
Server Error
404 - File or directory not found.
The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Information Security Program

Microsoft's online Information Security Program defines how OSSC operates. The program has been independently certified by British Standards Institute (BSI) Management Systems America as being compliant with ISO/IEC 27001:2005. To view the ISO/IEC 27001:2005 certificates, see the Certificate/Client Directory Search Results page.

The Information Security Program organizes security requirements into three top-level domains: Administrative, Technical, and Physical. The criteria in these domains represent the basis from which risk is managed. Starting with the safeguards and controls identified in the domains and their subcategories, the Information Security Program follows the ISO/IEC27001:2005 framework of "Plan, Do, Check, Act."



Operational Compliance

The Microsoft online services environment must meet numerous government-mandated and industry-specific security requirements in addition to Microsoft's own business-driven specifications. As Microsoft online businesses continue to grow and change and new online services are introduced into the Microsoft cloud, additional requirements are expected that could include regional and country-specific data security standards. The Operational Compliance team works across operation, product, and service delivery teams and with internal and external auditors to ensure Microsoft is in compliance with relevant standards and regulatory obligations. The following list presents an overview of some of the audits and assessments that the Microsoft cloud environment undergoes on a regular basis:

- **Payment Card Industry Data Security Standard** – Requires annual review and validation of security controls related to credit card transactions.
- **Media Ratings Council** – Relates to the integrity of advertising system data generation and processing.
- **Sarbanes-Oxley** – Selected systems are audited annually to validate compliance with key processes related to financial reporting integrity.
- **Health Insurance Portability and Accountability Act** – Specifies privacy, security, and disaster recovery guidelines for electronic storage of health records.
- **Internal audit and privacy assessments** – Assessments occur throughout a given year.

Meeting all these audit obligations became a considerable challenge at Microsoft. Upon studying the requirements, Microsoft determined that many of the audits and assessments required evaluation of the same operational controls and processes. Recognizing the significant opportunity to eliminate redundant efforts, streamline processes, and proactively manage compliance expectations in a more comprehensive manner, OSSC developed a comprehensive compliance framework. This framework and associated processes are based on a five-step methodology represented in the following illustration:

Microsoft Azure Cloud Security

One of the successes of having implemented this program is that Microsoft's cloud infrastructure has achieved both SAS 70 Type I and Type II attestations and ISO/IEC 27001:2005 certification. This achievement demonstrates Microsoft's commitment to delivering a trustworthy cloud computing infrastructure because having:

- The ISO/IEC 27001:2005 certificate validates that Microsoft has implemented the internationally recognized information security controls defined in this standard, and
- The SAS 70 attestations illustrate Microsoft's willingness to open up internal security programs to outside scrutiny.

PUBLIC

Slide 77

Microsoft Azure Cloud Security

Security and regulatory compliance

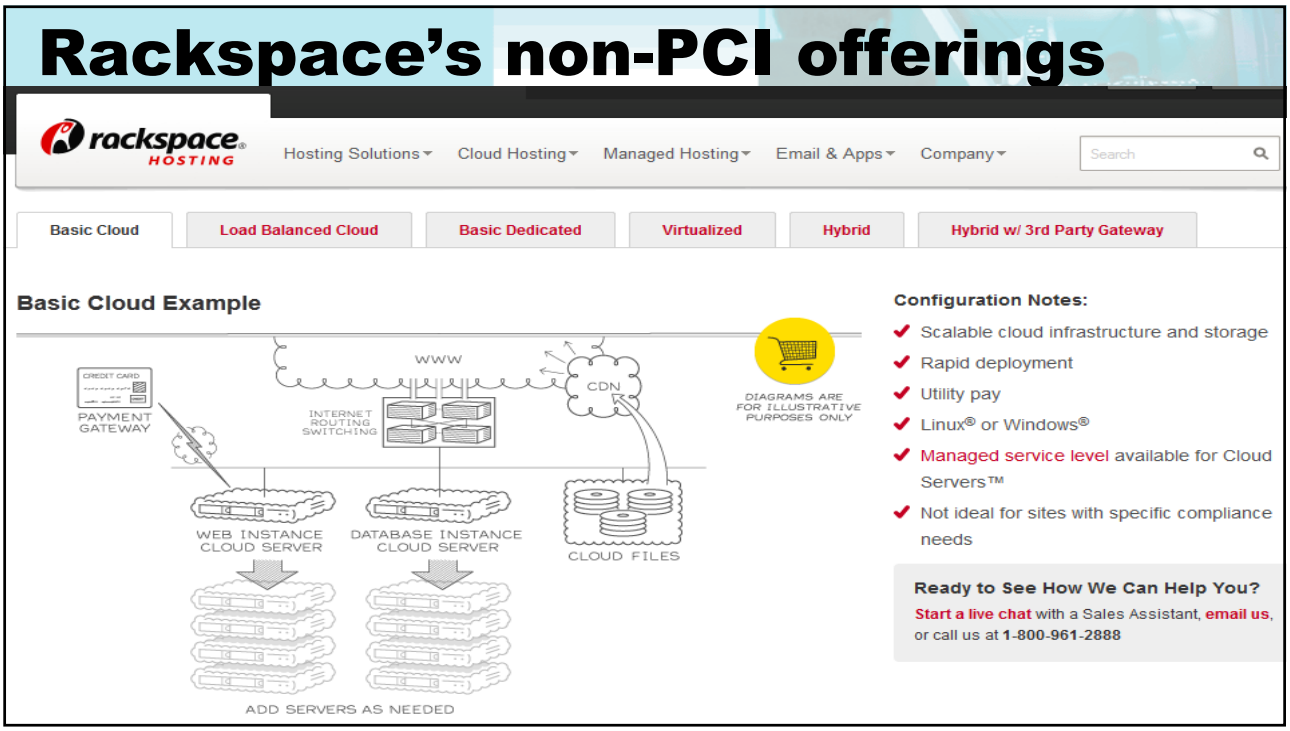
As a service provider, Microsoft must comply with regulatory requirements of the governmental entities within whose jurisdictions Azure operates, along with industry regulations that cover many companies in specific fields. Microsoft's compliance framework is designed to address this challenge. The security for Microsoft's cloud infrastructure is managed by the Online Services Security and Compliance team, which maintains the security control framework and develops policies and programs for ensuring compliance and managing security risks.

The Microsoft cloud undergoes annual audits for PCI DSS, SOX and HIPAA compliance, as well as internal assessments throughout the year. The Microsoft cloud has obtained ISO/IEC 27001:2005 certification and SAS 70 Type I and II attestations.

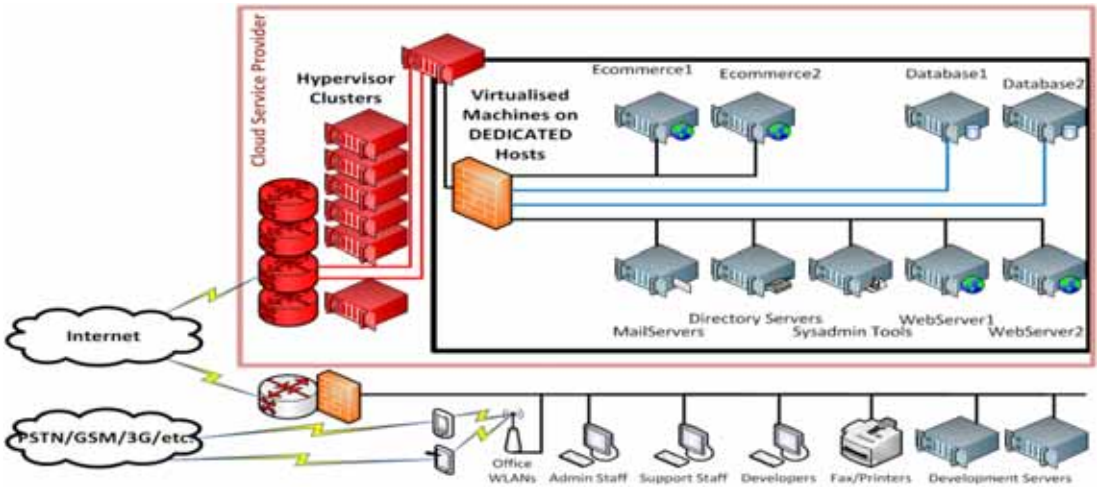
PUBLIC

Slide 78

Rackspace's non-PCI offerings



3. Dedicated Machines



BRIDGE POINT "SECURE NETWORKING"

Slide 80

Rackspace Enhances Security with PCI Accreditation

+1 Tweet

Date: August 13th, 2009

LONDON - 13 August, 2009 - Rackspace® Hosting, the world's leader in hosting, today announces it is Payment Card Industry (PCI) Data Security Standard (DSS) compliant, meeting a comprehensive set of security requirements designed to protect cardholder information.

PCI DSS certification as a Level 1 Service Provider reinforces Rackspace's ability to provide secure services to its customers, particularly in the E-Commerce sector, where the need to protect cardholder information is critical. Rackspace can now provide a more comprehensive set of products and services, which can help enable a customer to better meet their compliance requirements. The Rackspace PCI service is backed by Rackspace's Fanatical Support® which offers 24x7x365 support.

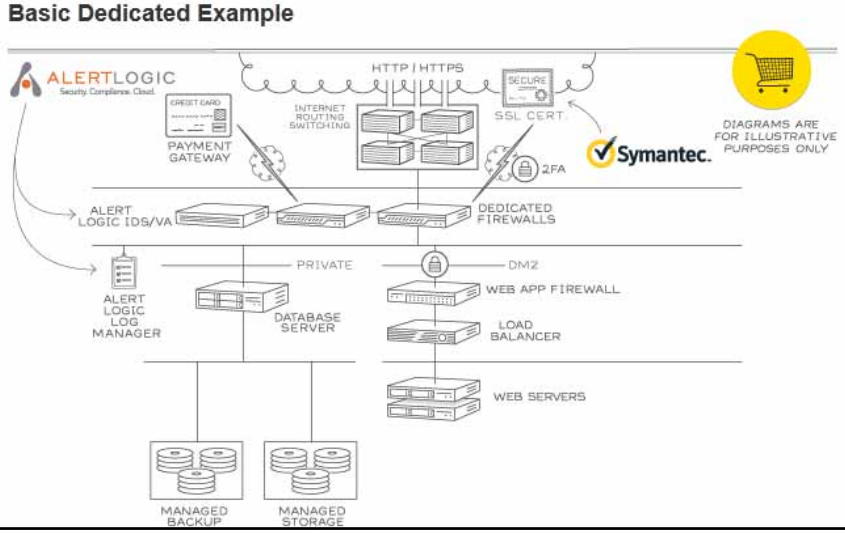
The scope of Rackspace's PCI service provider accreditation covers the following:

Physical security for
UK and US data centres
US and UK offices
Network infrastructure (routers and switches)
Employee access to network devices

Rackspace's dedicated hardware

Basic Cloud | Load Balanced Cloud | Basic Dedicated | Virtualized | Hybrid | Hybrid w/ 3rd Party Gateway

Basic Dedicated Example

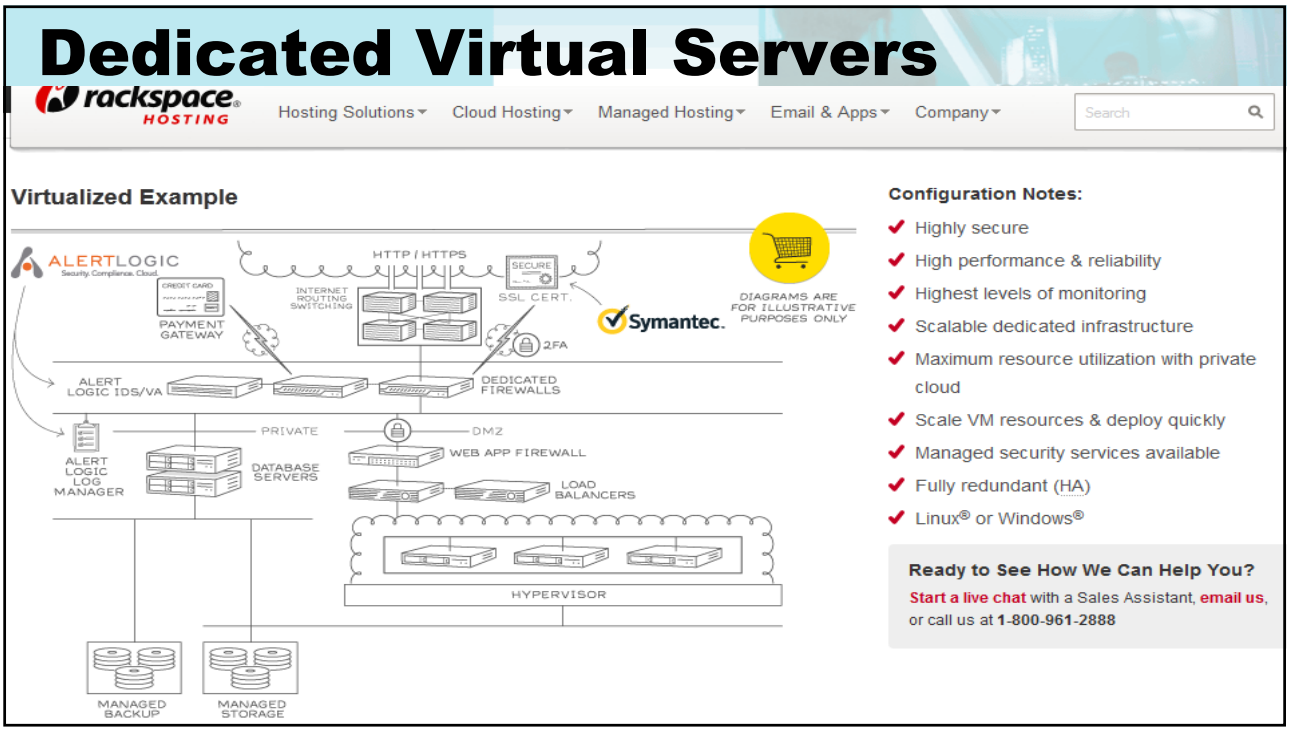


Configuration Notes:

- ✔ Highly secure
- ✔ Scalable dedicated infrastructure
- ✔ High performance & reliability
- ✔ Managed security services available
- ✔ Fully redundant (HA)
- ✔ Linux® or Windows®
- ✔ Highest levels of monitoring

Ready to See How We Can Help Yo

Start a live chat with a Sales Assistant, ema
or call us at 1-800-961-2888


Dedicated Virtual Servers
rackspace HOSTING
Hosting Solutions
Cloud Hosting
Managed Hosting
Email & Apps
Company
Search
Virtualized Example
ALERTLOGIC
HTTP / HTTPS
SECURE
SSL CERT.
INTERNET ROUTING SWITCHING
PAYMENT GATEWAY
Symantec.
2FA
DIAGRAMS ARE FOR ILLUSTRATIVE PURPOSES ONLY
ALERT LOGIC IDS/VA
DEDICATED FIREWALLS
PRIVATE
DMZ
WEB APP FIREWALL
ALERT LOGIC LOG MANAGER
DATABASE SERVERS
LOAD BALANCERS
HYPERVISOR
MANAGED BACKUP
MANAGED STORAGE
Configuration Notes:
Highly secure
High performance & reliability
Highest levels of monitoring
Scalable dedicated infrastructure
Maximum resource utilization with private cloud
Scale VM resources & deploy quickly
Managed security services available
Fully redundant (HA)
Linux® or Windows®
Ready to See How We Can Help You?
Start a live chat with a Sales Assistant, email us, or call us at 1-800-961-2888


Achieving PCI DSS Compliance with Rackspace
rackspace

PCI Compliance Requirements

REQUIREMENT 1.1 TO 1.1.1

Formal Process for Approving and Testing all Network Connections and Change to the Network Configuration

Overview

Implement policies and processes for approving and testing all connections and changes to the network. The policy should list all network devices involved in the data flow.

Responsibility

Requirement can be achieved by incorporating the formal process into the customer security policy. Customers are responsible for implementing formal security controls, including a security policy and associated processes and procedures to adhere to the security policy.

REQUIREMENT 1.1.2

Current Network Diagram with All Connections to Cardholder Data, Including Wireless Networks

Overview

Network diagram and topology documents

Responsibility

Customer is responsible for mapping the data flow of card holder data across the network. Rackspace can provide network diagram upon request.

REQUIREMENT 1.1.3

Requirement for a Firewall at each Internet Connection and between DMZ

Overview

Minimise the risk of malicious access to the internal network by implementing a firewall at each internet connection

REQUIREMENT 1.1.3

Requirement for a Firewall at each Internet Connection and between DMZ

Overview

Minimise the risk of malicious access to the internal network by implementing a firewall at each internet connection and between DMZ. This should include restricting inbound and outbound traffic to that which is necessary for the cardholder data environment, secure and sync up firewall and router configurations, prohibit internal addresses from being passed to the internet, allow only the necessary protocols, stateful packet inspection, implementing NAT, security of mobile devices connecting to cardholder environment.

Responsibility

Customer is responsible for incorporating this requirement as a standard as part of the customer security policy. Rackspace will configure the firewall for this requirement, upon request from the customer.

REQUIREMENT 1.1.4

Description of Groups, Roles and Responsibilities for Logical Management of Network Components

Overview

Clear assignment of groups, roles and responsibilities can be incorporated into the customer security policy

Responsibility

In a typical Rackspace PCI customer hosted environment, Rackspace manage the following devices:

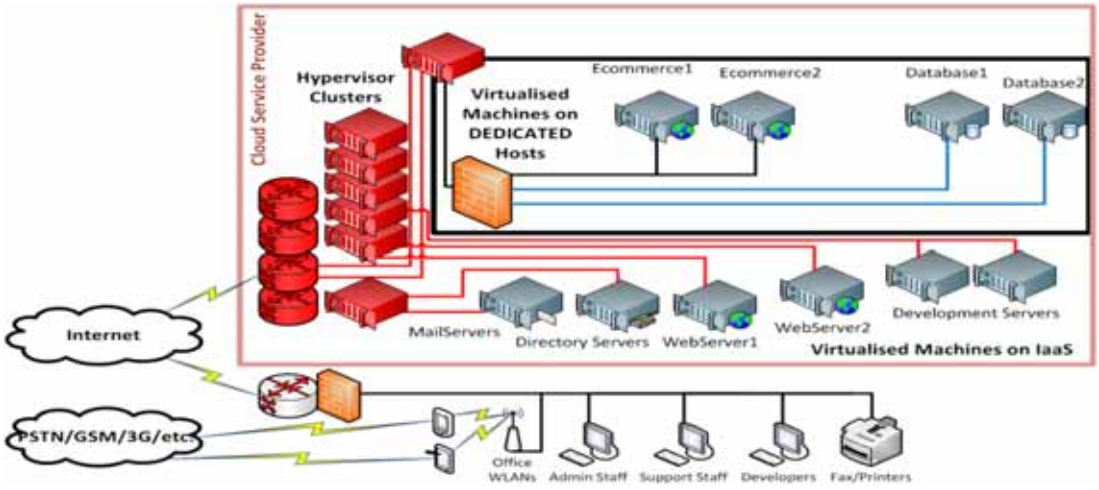
- IDS
- Load Balancer
- Firewall (customer can make firewall access rule changes via the customer portal)

Rackspace support team and selected customer personnel also have access to manage the following devices:

- Servers

Any changes to the customer hosted environment should be initiated by the customer via phone or ticket. All changes to the customer environment should be recorded in a ticket by the Rackspace support team and by the customer. There may be occasions when Rackspace are required to make changes to the corporate infrastructure which may affect a customer hosted environment, however all changes are communicated prior to any changes being performed.

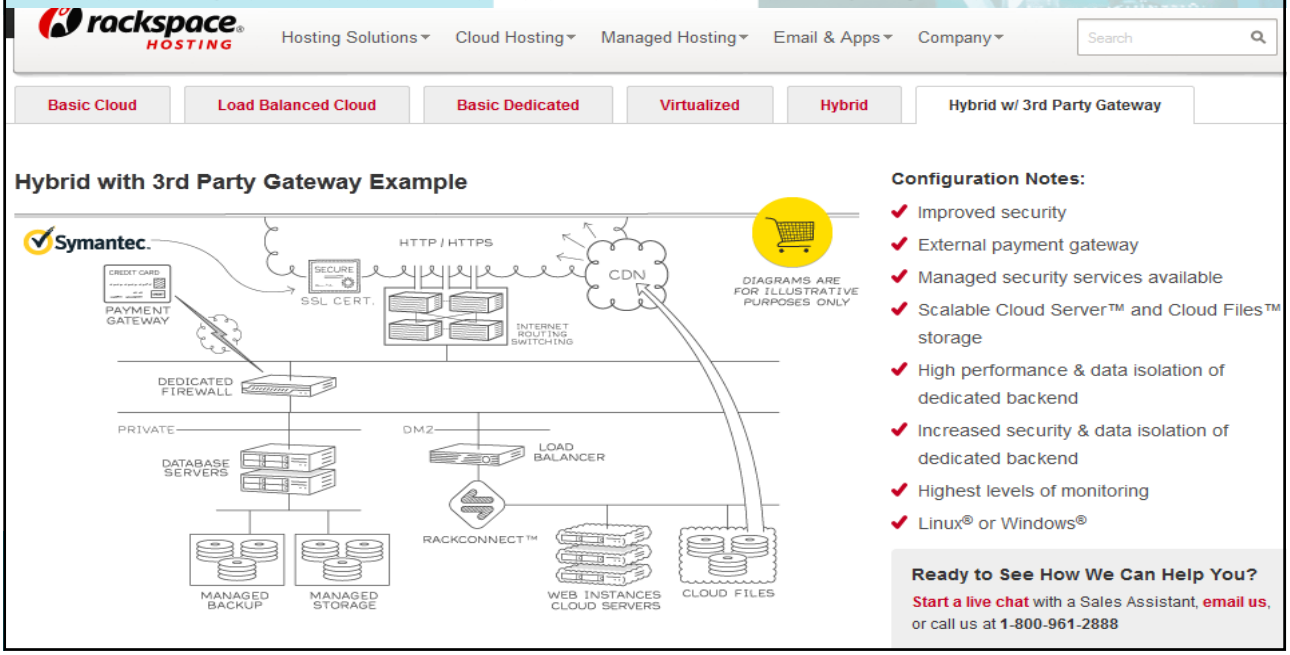
4. Mixed Dedicated + Public Cloud



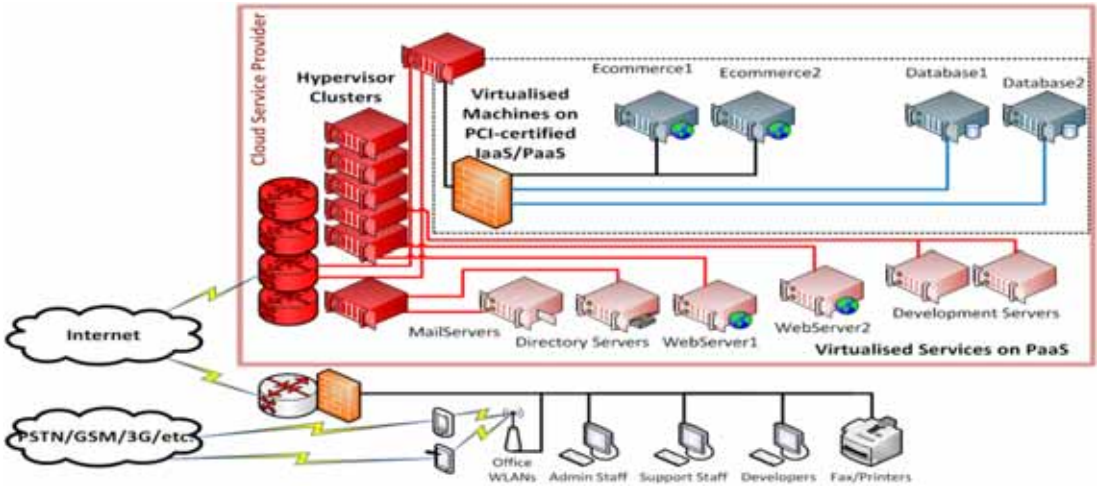
BRIDGE POINT "SECURE NETWORKING"

Slide 87

Dedicated Data + Public Cloud Web



5. PCI-certified IaaS (+ any others)



BRIDGE POINT "SECURE NETWORKING"

Slide 89

What Amazon Web Services product offerings support storage, proce transmission of credit card data?

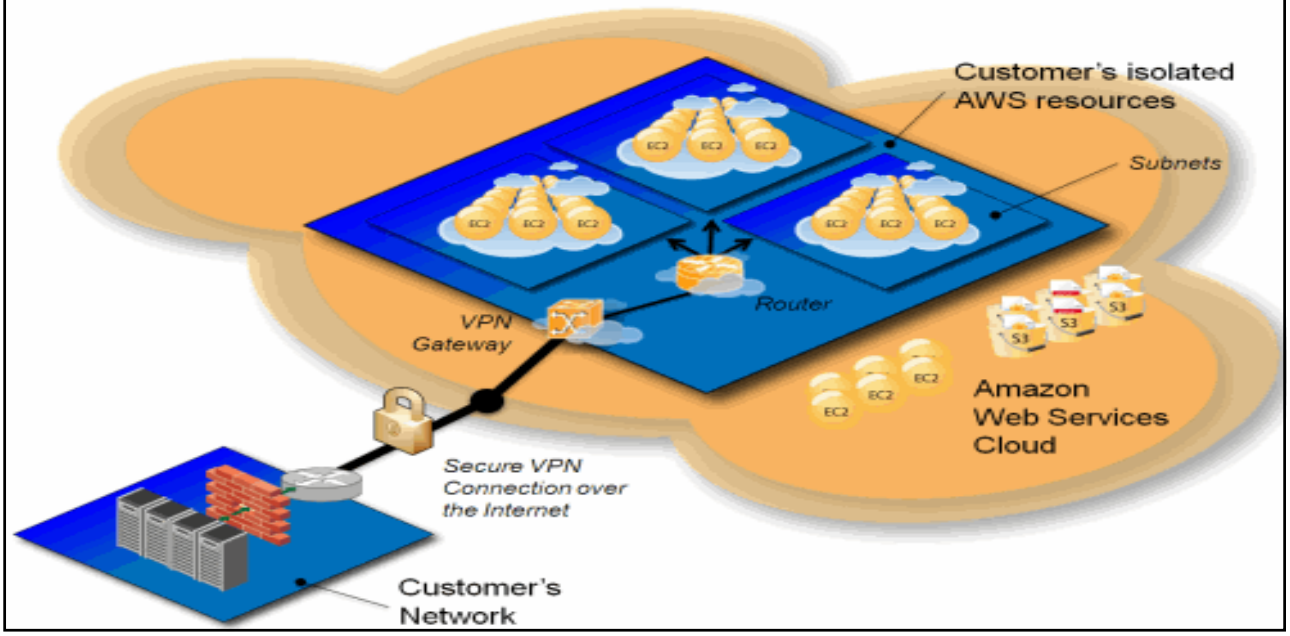
Services that support the processing, storage, and transmission of credit card data by a mercha provider have been validated as being compliant with PCI standards. These services include:

- Amazon Elastic Compute Cloud (EC2)
- Amazon Simple Storage Service (S3)
- Amazon Elastic Block Storage (EBS)
- Amazon Virtual Private Cloud (VPC)
- Amazon Relational Database Service (RDS)
- Amazon Elastic Load Balancing (ELB)
- Amazon Identity and Access Management (IAM)
- The underlying physical infrastructure and the AWS Management Environment

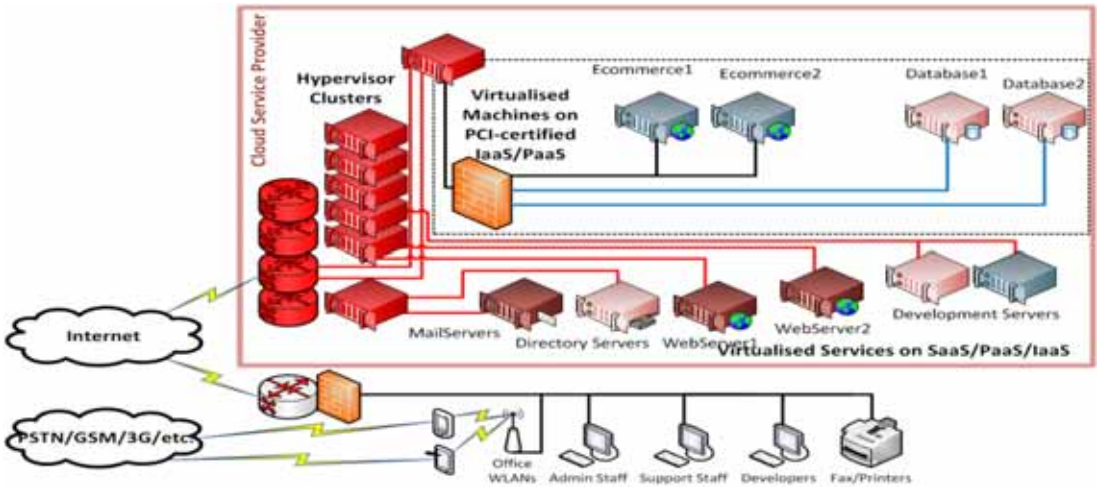
What does this mean to me as a PCI merchant or service provider?

Our PCI Service Provider status means that customers who use our services to store, process o cardholder data can rely on our PCI compliance validation for the technology infrastructure as th own compliance and certification, including PCI audits and responses to incidents. Our service p covers all requirements as defined by PCI DSS for physical infrastructure service providers. Movi cardholder environment to AWS can simplify your own PCI compliance by relying on our validate status. If your QSA currently needs additional supporting information, please contact us.

Amazon's Private + Public (All PCI)



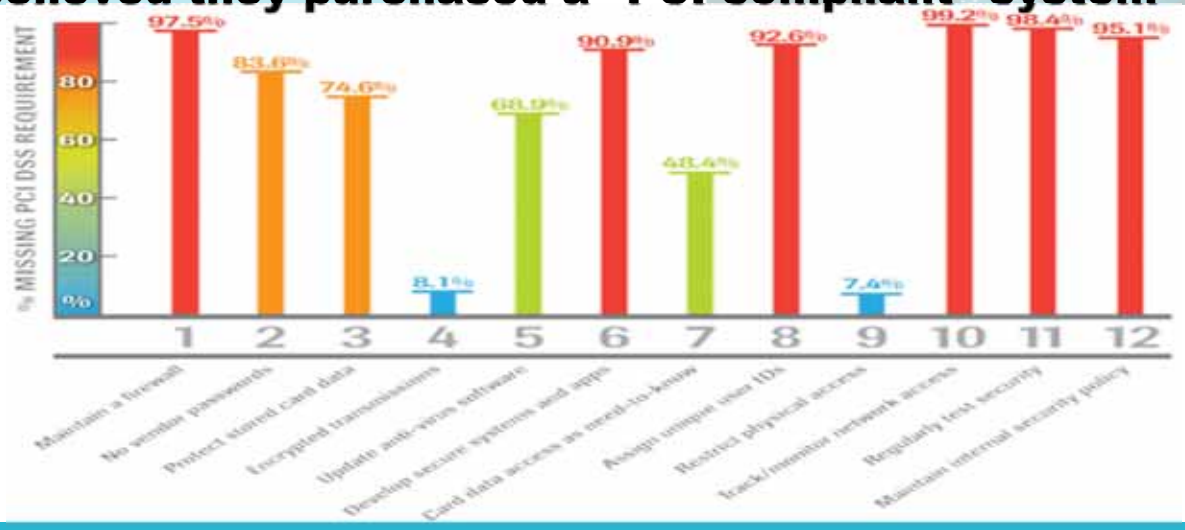
Everything!



BRIDGE POINT "SECURE NETWORKING"

Slide 92

Trustwave Global Security Report 2011 (p.12): 'believed they purchased a "PCI compliant" system'



PUBLIC

BRIDGE POINT "SECURE NETWORKING"

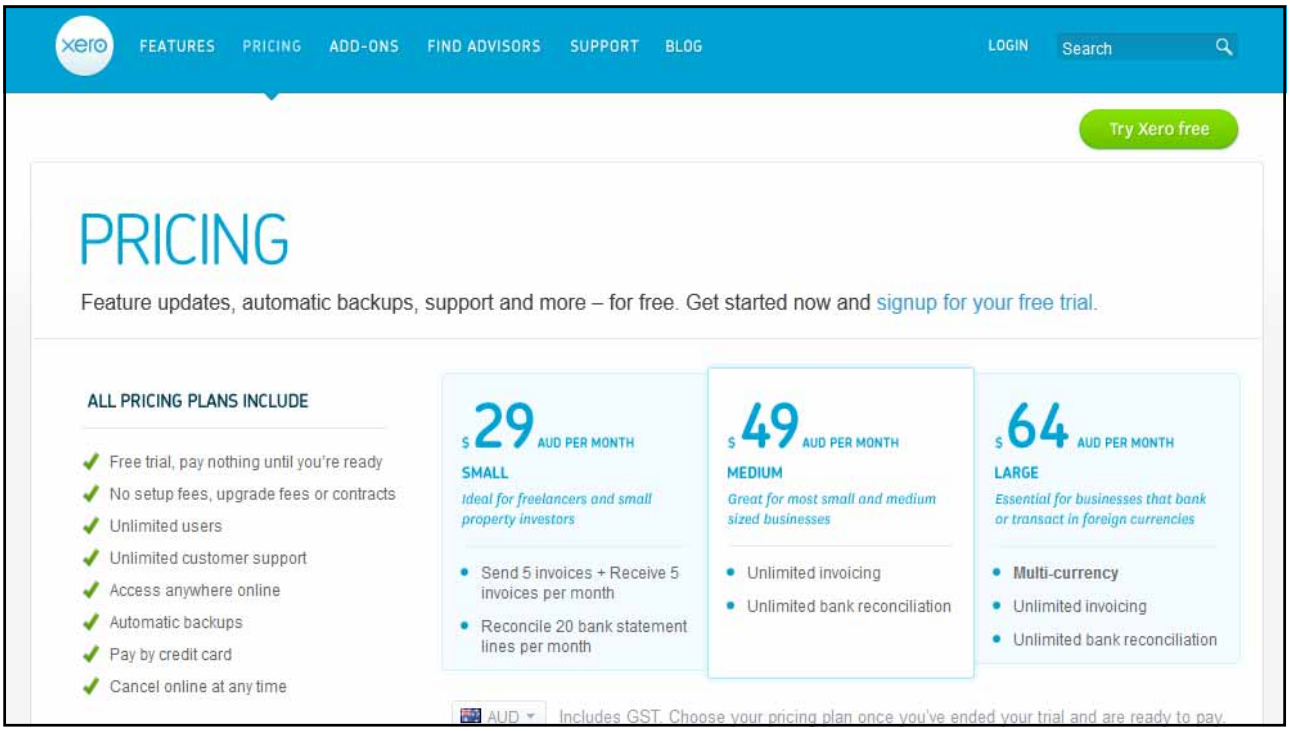
Slide 93

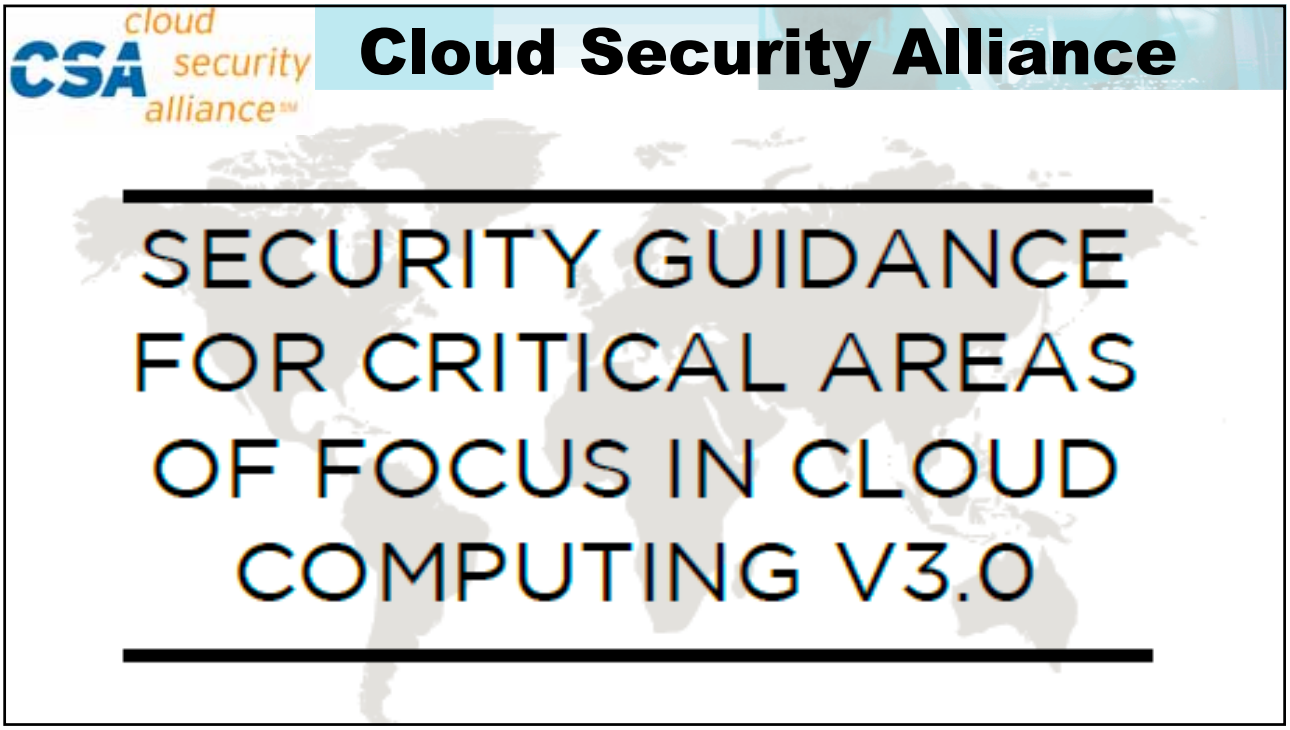
Where to go from here

- Deciding What, When, & How to Move to the Cloud
- Identify the asset you want to "vaporise"
  - Data
  - Applications/Functions/Processes
- Evaluate the asset
  - Evaluate the BUSINESS asset, not the IT asset

BRIDGE POINT "SECURE NETWORKING"

Slide 94


xero
FEATURES
PRICING
ADD-ONS
FIND ADVISORS
SUPPORT
BLOG
LOGIN
Search
Try Xero free
PRICING
Feature updates, automatic backups, support and more – for free. Get started now and signup for your free trial.
ALL PRICING PLANS INCLUDE
Free trial, pay nothing until you're ready
No setup fees, upgrade fees or contracts
Unlimited users
Unlimited customer support
Access anywhere online
Automatic backups
Pay by credit card
Cancel online at any time
$29 AUD PER MONTH
SMALL
Ideal for freelancers and small property investors
Send 5 invoices + Receive 5 invoices per month
Reconcile 20 bank statement lines per month
$49 AUD PER MONTH
MEDIUM
Great for most small and medium sized businesses
Unlimited invoicing
Unlimited bank reconciliation
$64 AUD PER MONTH
LARGE
Essential for businesses that bank or transact in foreign currencies
Multi-currency
Unlimited invoicing
Unlimited bank reconciliation
AUD
Includes GST. Choose your pricing plan once you've ended your trial and are ready to pay


cloud security alliance
CSA
Cloud Security Alliance
SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0

cloud security alliance℠

MISSION STATEMENT

To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.

98

About the Cloud Security Alliance

- *Global, not-for-profit organization*
- *Building best practices and a trusted cloud ecosystem*
- *Comprehensive research and tools*

Certificate of Cloud Security Knowledge (CCSK)

www.cloudsecurityalliance.org

Evaluate the asset

1. How would we be harmed if the asset became widely public and widely distributed?
2. How would we be harmed if an employee of our cloud provider accessed the asset?
3. How would we be harmed if the process or function were manipulated by an outsider?
4. How would we be harmed if the process or function failed to provide expected results?
5. How would we be harmed if the information/data were unexpectedly changed?
6. How would we be harmed if the asset were unavailable for a period of time?

Choose cloud deployment model

1. Public.
2. Private, internal/on-premises.
3. Private, external (including dedicated or shared infrastructure).
4. Community; taking into account the hosting location, potential service provider, and identification of other community members.
5. Hybrid. To effectively evaluate a potential hybrid deployment, you must have in mind at least a rough architecture of where components, functions, and data will reside.

Evaluate service models/providers

- Focus on the degree of control you'll have at each SPI (SaaS, PaaS, IaaS) tier to implement required risk management
- Sketch the potential data flow between
  - your organisation,
  - the cloud service,
  - and any customers/other nodes.
- Before making a final decision it's essential to understand whether, and how, data can move in and out of the cloud.

BRIDGE POINT "SECURE NETWORKING"

102

Stay Compliant

Ongoing compliance with PCI DSS – tasks:

TASK	*FREQUENCY*
Risk assessment, security awareness, key changes, penetration testing, review off-site backups, QSA assessment, etc	Annual, (+ major changes)
ASV and internal scans, wireless scans	Quarterly
File integrity checking	Weekly
Log and alerts review, other operational procedures	Daily

CSA cloud security alliance

103

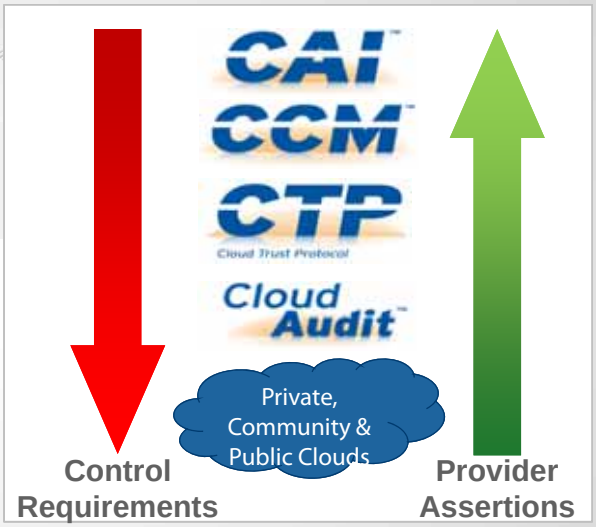
While we are *"in the cloud"*

Here are some additional CSA/cloud security resources…

104

CSA GRC Stack

Bringing it all together to peel back the layers of control ownership and address concerns for trusted Cloud adoption.



105

CSA CloudAudit

Cloud Audit
The A6 Working Group

- *Open standard and API to automate provider audit assertions*
- *Change audit from data gathering to data analysis*
- *Necessary to provide audit & assurance at the scale demanded by cloud providers*
- *Uses Cloud Controls Matrix as controls namespace*
- *Use to instrument cloud for continuous controls monitoring*

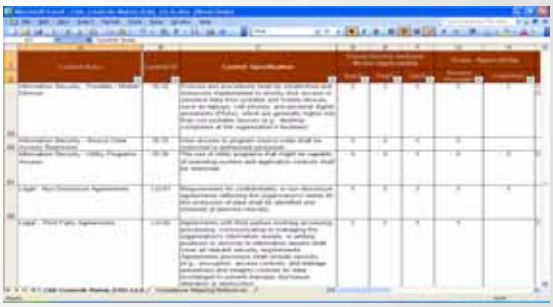
cloud security alliance

106

CSA Cloud Controls Matrix

- *Controls derived from guidance*
- *Mapped to familiar frameworks: ISO 27001, COBIT, PCI, HIPAA*
- *Rated as applicable to SaaS/PaaS/IaaS*
- *Customer vs Provider role*
- *Help bridge the "cloud gap" for IT & IT auditors*

CCM
Cloud Controls Matrix



https://cloudsecurityalliance.org/research/projects/cloud-controls-matrix-ccm/

cloud security alliance

cloud security alliance℠

CSA Australia

- Cloud Security Alliance, Australian Chapter.
- LinkedIn Group:
  http://www.linkedin.com/groups?gid=3966724

Founding Directors – CSA–AU

- Ben Chung (HP, NSW)
- Gary Gardiner (Check Point, QLD)
- Wipul Jayawickrama (Infoshield, QLD)
- Richard Keirstead (Ernst & Young, VIC)
- Craig Lawson (HP, QLD)
- Simon O'Brien (BPC, QLD)
- Archie Reed (HP, NSW)
- David Ross (BPC, QLD)
- Darren Skidmore (FIS, VIC)
- Tim Smith (BPC, QLD)
- Marcel Sorouni (BUPA, NSW)
- Michael Trott (BPC, QLD)
- Chad Walker (Infoshield, QLD)
- Marcus Wong (CBA, NSW)
- Jason Wood (CBA NSW)

PUBLIC

BRIDGE POINT "SECURE NETWORKING"

Slide 109

Areas of Interest

- Virtualisation Security;
- Jurisdiction, Legal and Privacy issues as particular to Australian states and territories;
- Identity Management; and
- Standards, Compliance, and Audit.

BRIDGE POINT "SECURE NETWORKING"

Slide 110

CSA-AU meeting THU 12:35 Norfolk

cloud CSA security alliance SM

CCSK™

Home

Certificate of Cloud Security Knowledge

Cloud computing is being aggressively adopted on a global basis as businesses seek to reduce costs and improve their agility. And one of the critical needs of the industry is to provide training and certification of professionals to assure that cloud computing is implemented responsibly, and with the appropriate security controls.

The Cloud Security Alliance has developed a widely adopted catalogue of security best practices, the "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1". In addition, the European Network and Information Security Agency (ENISA) whitepaper "Cloud Computing: Benefits, Risks and Recommendations for Information Security" is an important contribution to the cloud security body of knowledge.

The Certificate of Cloud Security Knowledge (CCSK) provides evidence that an individual has successfully completed an examination covering the key concepts of the CSA guidance and ENISA whitepaper.

Examination Fee

The CCSK examination costs US$295. This entitles you to attempt the test up to two times. If necessary, additional test attempts can be purchased for US$295 each.

cloud security alliance SM

Security Guidance for Critical Areas of Focus in Cloud Computing V2.1

Any questions?

BRIDGE POINT "SECURE NETWORKING"

115

Did I mention… ?

- http://www.linkedin.com/groups?gid=3966724
- https://chapters.cloudsecurityalliance.org/australia/

BRIDGE POINT "SECURE NETWORKING"

Slide 116